UiO : Institutt for informatikk
Det matematisk-naturvitskaplege fakultet

Development of a Lab Experiment for Intrusion Detection System in Wireless Body Area Networks

Santosh Maharjan, masteroppgåve våren 2013

Development of a Lab Experiment for Intrusion Detection System in Wireless Body Area Networks

Santosh Maharjan

23rd May 2013

Preface

This research work has been carried out for fulfilling requirement of my Master's Degree on Network and System Administration at University of Oslo. The thesis is accomplished in four months time. The platform for the thesis is provided by Norwegian Research Center and is conducted as a part of ASSET project that has been launched by Norwegian Research Center. Every infrastructure needed are provided by the Norwegian Research Center.

The study is on security system present for the WBAN technology deployment in relation to e-health system. Any compromise in information security in e-health might be paid by a patient life. An attempt is made to figure out what are the security threats in the WBAN and what detection and prevention tools do we have.

Setting up platform for conducing experiments is one of the important aspect of this work. Experiments are carried on a simulator and real hardware. DoS attack is one of the simplest but most devastating attacks in e-health system. There exits other forms of attack as well that are equally fatal. Ironically, we have very limited security system to mitigate those attacks.

This thesis might be helpful for those who think of implementing the WBAN technology like ZigBee application. It might pave a solid ground for the students and security professionals who think of working with security system in hot and new technology like the WBAN. For rest who are interested in security system, might find it interesting to know current security system developed till date for the WBAN technology.

Acknowledgment

First and foremost, I would like to express my sincere gratitude to my supervisors Senior Research Scientist Habtamu Abie and Lecturer Tore Moller Jonassen for their prolonged support, motivation and guidance throughout my thesis work. This thesis work would not have accomplished without their guidance.

I am equally thankful to Associate Professor Kyrre Begnum for the motivation and guidance he has been providing since the beginning of the work. His thesis specific instruction classes were the milestones to structure this thesis.

I am also grateful to Associate Professor Harek Gaugerud for his support and guidance. He has been always there to bolster and pave path whenever needed.

I gratefully acknowledge the assistance and generosity of Senior Technical Analyst Joshua Wright. Without his help, I could not have arranged necessary devices for performing intended experiments. Likewise, I am also thankful to Lead Application Engineer Michael Healy for providing continuous support needed for configuring Shimmer devices.

I would also like to thank Assistant Research Director Wolfgang Leister for providing information about ASSET project, structuring thesis work and his friendliness.

I heartily appreciate the advice and support provided by Kashif Habib Sheikh, PhD Student.

My sincere gratitude also goes to my colleague Yareed Bernamu Weldegiorgis for assisting me setting up lab infrastructure for the research and Sudhir Pandey for every technical help and support.

Last but not the least, I am equally indebted to my family and friends Sanju Silwal, Anjana Mulepati, Namrata Pradhan, Deepak Bista, Saroj Upadhya, Sudeep Karki and Nishes Joshi for providing me emotional support and inspiration to accomplish my research work up to mark.

Acronyms

- AES - Advance Encryption Standard
- AIDPS - Adaptive Intrusion Detection and Prevention System
- AODV - Ad-hoc On-demand Distance Vector
- AP - Access Point
- ASSET - Adaptive Security for Smart Internet of Things in e-Health
- CRC - Cyclic Redundancy Check
- CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance
- DARPA - Defense Advanced Research Projects Agency
- DoS - Denial of Service
- EAP - Extensible Authentication Protocol
- FIM - File Integrity Monitoring
- HIDS - Host Based Intrusion Detection System
- IC - Integrity Check
- ICMP - Internet Control Message Protocol
- IDS - Intrusion Detection System
- IEEE - Institute of Electrical and Electronics Engineer
- GTS - Guaranteed Time Slot
- IP - Internet Protocol
- IPS - Intrusion Detection System
- IPsec - Internet Protocol Security
- ISM - Industry, Scientific and Medical
- IV - Initialization Vector
- MAC - Medium Access Control

- MD5 - Message Digestion 5
- NGIPS - Sourcefire Next-Generation Intrusion Prevention System
- NIDS - Network Based Intrusion Detection System
- NWK - Network
- OISF - Open Information Security Foundation
- OSI - Open System Interface
- OTA - Over-the-Air
- PAN - Private Area Network
- PSK - Pre-Shared Key
- RADIUS - Remote Authentication Dial-In User Service
- RPM - Red-Hat Packet Manager
- SIEM - Security Information and Event Management
- SIM - Security Information Management
- SMA - Sub Miniature
- SSID - Service Set Identifier
- SSH - Secure Shell
- SSL - Secure Socket Layer
- SWATCH - Simple Watcher
- TKIP - Temporal Key Integrity Protocol
- URI - Universal Resource Identifier
- VoIP - Voice Over Internet Protocol
- WBAN - Wireless Body Area Network
- WEP - Wired Equivalent Protection
- WPA - Wifi Protected Access
- WLAN - Wireless Local Area Network
- WPAN - Wireless Private Area Network
- WSN - Wireless Sensor Network
- XOR - Exclusive OR

Abstract

With the advent of sophisticated technology and associated indubitable benefits, the wireless network is gaining popularity day by day. Still there exists numerous security challenges and to overcome these, different researches are being carried on. This suggests that the wireless security is still in nascent stage and requires further development. The new wireless technologies like Wireless Body Area Network, thus provides tough challenges to security professionals. Wireless Body Area Network (WBAN) technology has been center of attraction in e-health system. In this system, data security breach might even cost lives of patients, so it alarms the need for highly reliable security system. This thesis is pivoted on security vulnerabilities in Wireless Body Area Network and mitigation tools and techniques to get rid of them. The study corresponds with security concern of Adaptive Security for Smart Internet of Things in e-Health (ASSET)project that has been launched by Norwegian Research Center. The thesis enlightens ASSET with different types of security threats that exist in wireless network, specifically on WBAN. It provides ASSET an infrastructure setup to facilitate security analysis in its network environment. ZigBee network, an instance of the WBAN is deployed as experimental platform. Experiments are performed in the OPNET network simulator and ASSET laboratory, consisting of different types of sensor devices. The study shows DoS attack and message replay attack are easily accomplished and prevalent in WBAN. However, security system to prevent them are under development. Finally, the thesis provides ASSET a platform to perform security analysis on WBAN deployment.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

This thesis is carried out as a part of the project: Adaptive Security for Smart Internet of Things in e-Health (ASSET). The project has been launched by Norwegian Research Center. It is primarily focused on the risk-based adaptive security for Internet-of-Things (IoT) in realm of e-health system. The research is founded on Game Theory and Context-Awareness with view of boosting up the security level [5]. This security concern of the ASSET in e-health system is the ground of this study.

Recently, the deployment of e-health system has been attracted towards Wireless Body Area Network (WBAN) technology. The primary reasons behind inclination are: lower power consumption by WBAN devices and low implementation cost [6]. Despite the demand for WBAN is rapidly increasing, the security system developed for WBAN is still in embryonic stage. However, different security critical data communication has been deployed in this type of network. One of such critical deployments is data communication in e-health system. Data that flow in e-health system are so critical that any compromise on such data might be paid by lives of the patients. This alarms for the need for reliable security system in WBAN technology.

The security issues in wireless network, have been a topic for investigation for the security professionals. The ever present randomity and unpredictability of wireless network traffic are the primary obstacles in developing a single common standard solution for the wireless security breaches. Different wireless standards (802 family) have been developed and revised to assure better reliability and security on wireless network. Despite in-depth researches that have been carried out, the security threats are still prevailing. This is because of the novel threats that are introduced by the hackers and attackers on wireless network. Hackers and attackers find comparatively easier path to intrude into the wireless network due to its easy accessibility feature.

The study discusses on different types of wireless attacks that an intruder might come up with. The primary focus is paid on Wireless Body Area Network security issues. Daniel-of-Service (DoS) attack is the most common

attack in any wireless network. Thus, experiments are focused on different types of DoS attacks in the WBAN. Sniffing, capturing network traffic and replay attack are other considerations of this research. Experiments are performed on two platforms. In the ASSET laboratory, tests are carried out in a ZigBee network, one of the demanding implementations of the WBAN standard. Sniffing, packet capture, replay attack and selective DoS attacks are experimented in the real hardware. Jammer DoS attack and misbehaving node DoS attack are analyzed through a simulator named: OPNET Modeler Wireless Suite version 17.5.

The research finds out that DoS attacks can easily be created on 802.15.4 or ZigBee network. Similarly, sniffing, packet capture and replay attack are also possible. However, it requires special hardware and firmwares to accomplish these attacks. The study provides knowledge about these different hardware devices that assist in creating attack scenarios. In addition, it delivers idea about different sensor devices and related firmwares that can be deployed to analyze 802.15.4 traffic. Details on creation of attacks and results with the analysis are presented in the following chapters.

Initially, the objective of this research was to analyze the different adaptive intrusion detection and prevention system developed for WBAN technology. Unfortunately, no such tools are found developed for WBAN network. Attempts were made to deploy some of the wireless security tools developed for Wireless Local Area Network (WLAN) technology, but could not produce the result due to some circumstances. These circumstances are discussed in Discussion Chapter along with limitation of this research.

1.2 Problem Statement

Security in data communication in e-health system cannot be compromised or else it may lead to severe adverse effect, like death of the patients. The reasons behind such effects can be: modified critical data about blood pressure, heart bits etc. and unavailability of timely data. Ironically, the security tools development are in nascent stage.

1.3 Objective and Significance

Resolving the issues mentioned below are the objective and significance of this research.

1. the WBAN has emerged as new wireless technology, where the data security is even more crucial. Thus, what can be the likely security breaches in the WBAN in relation to e-health service and how can they be detected and avoided?

2. A handful of Wireless Intrusion Detection and Prevention System do exist til date. All of them are developed for WLAN standard. Can these tools operate in the WBAN sensor network? If so, what is the best available tool for the WBAN standard when it involves e-health

security issues? If not, what further enhancement these tools must be embedded with, to assure their deployment; in the realm of the WBAN e-health service?

1.4 Structure of Study

The study has been discussed under six chapters. The first chapter, Introduction, provides scope, significance and quick overview of important aspects of the research. The second chapter, Background and Literature, discusses on related work carried out previously and theoretical base that are necessary to formulate ground for experiments and analysis. In the third chapter, Approach, preliminary plans and procedures to resolve problem statements and meet the objective of the study, are mentioned. The fourth chapter, Result and Analysis, presents the ways the experiments are conducted, results obtained and analysis of the results. The fifth chapter, Discussion, enlightens about the findings and significance of the research. It also addresses about shortcomings and complications encountered and shares the knowledge and lesson gained from this thesis work. Finally, in the sixth chapter, Conclusion, important portions of the study are summarized along with possible future extensions of this work.

Chapter 2

Background and Literature

This portion of the report discusses on related background theories in wireless network. The background theory starts with related work accomplished previously. Then, it continues further with highlighting on security issues in wireless network and different wireless standards we have. WLAN and Wireless Body Area Network (WBAN) are discussed in more details, with respective standards, security features and security flaws encompassed by them. The section also provides short overview of the popular wireless network simulators. At the end, the background theory discusses on different intrusion detection mechanisms and tools, focusing on real time adaptive features.

2.1 Related Work

This chapter presents the different relevant researches or experiments carried on security vulnerabilities in the WBAN or 802.15.4 network. The chapter also includes some relevant researches conducted on security tools developed or proposed in order to combat the security threats in the WBAN network.

Security Exploitation in WBAN

Sang Shin Jung in his Master's Thesis [7] demonstrated the different possibilities to attack wireless sensor network. He presented how beacon-enabled 802.15.4 network is open to availability and integrity breaches. In his experiment, he implemented Tmote Sky motes devices as sensor nodes in beacon-enabled mode. The network consisted of a Private Area Network (PAN co-coordinator) and other three nodes. These end devices used to send temperature and humidity related data to the *Coordinator*. Among the three end nodes, a node was configured to function as malicious node. He has demonstrated how synchronization attack degrades the throughput of PAN coordinator. Secondly, Jung talked about DoS attack. Jung presented how Guaranteed Time Slot (GTS) deallocation request from the malicious node consumes the network resource, lowering throughput of other end nodes. Next, he performed impersonation attack through eliminating GTS descriptor from malicious attack. The other nodes that waited for their

GTS, kept on waiting and waiting. This was mentioned about another DoS attack. In false data injection attack, he exhibited that misbehaving nodes injecting false data in the network in the name of other nodes. Further, Jung presented the two other forms of DoS attack through GTS request packet. In addition Jung talked about different pitfalls those exist on 802.15.4 network. He then recommends the possible preventive mechanisms to control mentioned attack. Mostly they were focused on authentication of GTS request through unicast authentication procedure.

Joshua Wright [8] has developed a open source firmware named KillerBee based on python language. The tool is used to generate different attacks on 802.15.4 network, precisely in ZigBee network. In his video presentation, he demonstrated how KillberBee configured specific device could generate different attacks in the ZigBee network. Message sniffing and then making replay attacks were the primary concerns. The implementation of KillerBee is confined within particular sensor device named Atmel AVR RAVEN or RZUSBSTICK [9] used in ZigBee network. Other sensor devices like Telosb Tmote Sky can also be configured with KillerBee but for the full functionality may not be supported. The KillerBee tool is found deployed in many other researches as a packet sniffer.

Several other researches are found carried on security vulnerabilities on 802.15.4 network. An article on Jamming the 802.15.4 network [10], by a group of students at Virginia University demonstrated their research and presented different ways of jamming the 802.15.4 network. They proposed different techniques on combating the different jamming attack if the attacks are being conducted by the devices similar to the devices in use. They implemented a network of MICAz mote devices in their work. Colin P. O'Flynn has also published an article [11] on jamming attacks on 802.15.4 network. He conducted his experiments on specific transceiver named Atmel AT86RF231. Colin has discussed on different ways of jamming ranging from selective channel jamming to whole network jamming. He also discussed on message specific jamming and presented the possibility of interfering to particular data flow in the network.

2.1.1 Simulation Work

Wireless sensor networks require different specific devices to conduct experiment on them. Thus, often the concentration is found paid on simulators. The OPNET simulator is widely used to simulate wireless sensor network. Jesus Manuel Gonzalez de Jesus had conducted his Master's Thesis on jamming attacks through implementation of OPNET 12.0 modulator [12]. The jamming attack study was made on 802.11 network. Through simulation he presented the different types of jamming attack on 802.11 network. He discusses on the four types of jammers those are present in the wireless communication, namely constant jammer, deceptive jammer, random jammer and reactive jammer. His thesis work was more pointed at implementing Opnet Modeler simulation tool to simulate jamming attacks.

Doddapaneni Krishna Chaitanya and Arindham Ghosh from Middlesex University performed the similar DoS attack tests in The OPNET simulator

16 [13]. They had designed a ZigBee network with ten sensor nodes, a ZigBee router and a ZigBee coordinator. Their simulation experiments were based on the parameters internal arrival time and packet size. Through alteration on those parameters on one or more sensor nodes, they presented how the throughput and volume of traffic sent in the network affected. As an conclusion, they drew that coordinator node was more sensitive to DoS attack than router node.

2.1.2 WBAN Security Tools

A number of researches and tests are conducted in designing the intrusion detection system for the WBAN. However, most of the researches are still confined to propose the models but no specific tools have been developed. The security systems lack specific tools that can be applied to detecting intrusion detection system in the WBAN. A group of five students Gjovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer and Richard A. Kemmerer, at University of California had designed intrusion detection tool for AODV protocol based ad hoc wireless network [14]. The tool developed by them could spoof the MAC address modifying the sequence number. The tool could also track the packets dropped by the intermediate misbehaving node, preventing the packets reaching to the final destination. Packet drops could of be different types based on the types of control data being sent. Their tool could also figure out the events of resource depletion attack in the network. According to them, resource depletion could be made possible by transmitting voluminous control packets. The tool could detect such attack as well. However, the tool developed by them was not brought into practice.

2.2 Wireless Standards

Depending upon the requirements, computer network is classified into different categories. It ranges from it's simple form of Private Area Network (PAN) to sophisticated Wide Area Network (WAN). Local Area Network and Metropolitan Area Network lie in between these two. Whether it is simple network (PAN) or the sophisticated network (WAN), there is provision of wireless data transmission. In PAN, wireless technologies are deployed in the form infrared, bluetooth data or other radio waves from simple APs. But on the other hand, complicated satellite technologies are implemented in WAN where radio signals can travel miles and miles cross the countries. Figure 2.1 represents the different wireless standards intended to meet different classes of network's requirements. However, the focus will be on WLAN and the WBAN standard discussed below.

2.3 Wireless Local Area Network

Wireless Local Area Network (WLAN) consists of communication devices interacting with each other through wireless channels. This network came

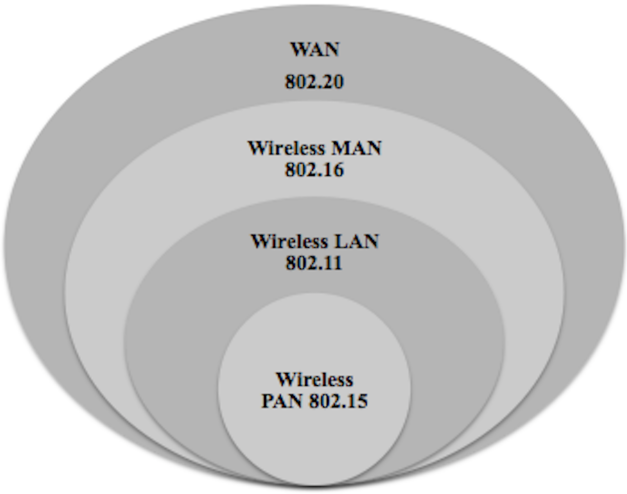


Figure 2.1: *Global Wireless Standards*

into existence so as to enhance the wired network with radio technology. With radio technology, wireless network facilitates user mobility during data connectivity and offers lowered cost over wired technology. For this reason, the wireless network is gaining popularity day by day and has been used as general-purpose connectivity in any business enterprises. WLAN provides solutions for small home network, cellular network and corporate network. Still, it is under continuous enhancement. The focuses are paid on quality of service, better security efficiency, shorter handover and increased throughput [15].

Despite the different advantages that the wireless network has over the wired network, it has different shortcomings in comparison with the wired network. Deterioration of power signal with distance to WLAN access point and interference in the wireless signal generated by the other devices operating on similar frequencies are the major drawbacks. Likewise, data rate in most wireless network seems comparatively lower than the wired network. "The wireless network lacks provision of transmitting and receiving data through the same channel at the same time" [15]. Moreover, the wireless network falls short of security assurance in contrast with the wired network.

Security issues in wireless network have always been of core interest in the field of computer network. The challenge is on providing efficient security solutions while maintaining scalability. The fundamental concern of WLAN security lies on authentication and authorization to secure network resources, data encryption and user data integrity [15]. In broad sense, authentication of users and access point, confidentiality, data integrity non-repudiation of origin and delivery, auditing and logging, denial of service prevention and traffic flow analysis prevention are the security concerns in a WLAN. To assure the availability solutions to these security issues, WLAN has defined different security levels and security framework components. Still, it lacks analysis on overall framework that may deploy different environments such as private, public and virtual network. Under such

conditions, the WLAN is expected to be embedded with possibility of roaming between such networks.

Out of seven layers of OSI module, in WLAN; security issues are dealt in layer two (Data-link Layer) and layer three (Network Layer) networks. At layer two, wired equivalent protection (WEP) is implemented. WEP is one of the security protocols based on wireless standard 802.11. It is supposed to assure that secured WLAN is as protected as wired network. Several such protocols have been developed for various WLAN technologies. Details on these protocols will be discussed later in this report. Likewise, the layer three security is supposed to facilitate user authentication, secure IP mobility and roaming among different domains. The security policies in WLAN can be implemented through host security, data driven attack prevention and organizational security policies [15].

2.3.1 WLAN Standards

In order to maintain compatible communication protocol among various networking devices in wireless network, IEEE has developed a common wireless standards for WLAN. The standard is known by 802.11 standard. The earlier version had security and limited bandwidth problems. Therefore; the standard has been revised and improved to accommodate the various bandwidth requirements of various users and enhance security. Common improved versions are 802.11b, 802.11a, 802.11g and 802.11n. However, some versions of wireless standards are not backward compatible with earlier versions. 802.11b is the earliest version of 802.11 WLAN standard. The latest version of the WLAN standard is 802.11n which can operate at 600 Mbps. 802.11a is not compatible with 802.11b while the other versions are compatible with 802.11b [4]. Recently, Wi.Fi (Wireless Fidelity) has established itself as de-facto standard for wireless communication in WLAN. Wi-Fi can provide service equivalent to wired service in terms of bandwidth. It operates in around 54 Mbps. In addition, Wi-Fi operates in ISM (Industry, Scientific and Medical) band and other user band which need not any license to use [16]. For these reasons, Wi-Fi has been widely deployed in WLAN. Table 2.1 provides the overview of different versions of wireless standard with accompanying bandwidth and technology used behind.

Table 2.1: *WLAN Standards [4]*

IEEE Standard	Frequency/ Medium	Speed	Topology	Transmission Range	Access Method
802.11	2.4 GHz RF	1 to 2 Mbps	Adhoc/ infrastructure	20 feet indoors	CSMA/CA
802.11a	5 GHz	upto 54 Mbps	Adhoc/ infrastructure	20 to 75 feet indoors	CSMA/CA
802.11b	2.4 GHz	upto 11 Mbps	Adhoc/ infrastructure	upto 150 feet indoors	CSMA/CA
802.11g	2.4 GHz	upto 54 Mbps	Adhoc/ infrastructure	upto 150 feet indoors	CSMA/CA
802.11n	2.4 GHz/ 5 GHz	upto 600 Mbps	Adhoc/ infrastructure	175+ feet indoors	CSMA/CA

2.3.2 WLAN Security

802.11 wireless standard has provided WLAN with benefits like mobility and productivity. Unfortunately, the wireless standard has several pitfalls. The wireless network has been playground for hackers and attackers. However, it does not mean that there exists no remedy to counteract such mischievous activities. One can mitigate the attacks and hacks in wireless network if the proper deployment of physical devices and security policies are implemented. Figure 2.2 shows different components of a wireless network with possible attack areas among them. And the following five ideas and techniques are found deployed to get rid of wireless-specific attack [17]:

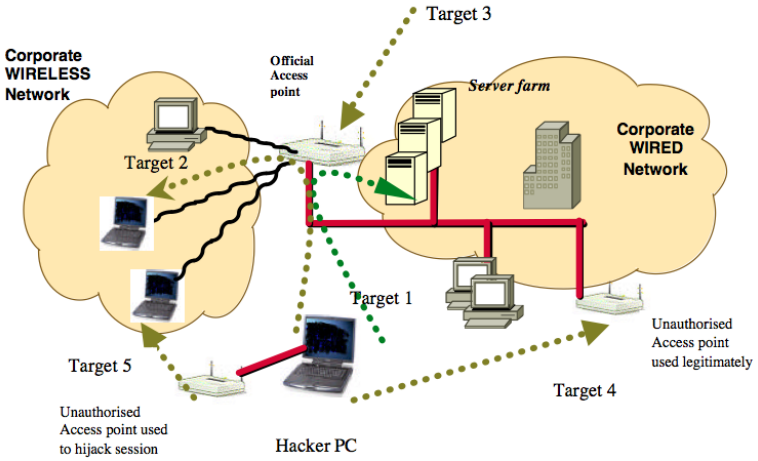


Figure 2.2: *Elements of Wireless Network with possible Attack Areas [1]*

1. **Discovery and Mitigation of Rogue APs and Vulnerabilities:** One of the primary reasons for wireless security pitfalls is allowing open connection to the wireless network. Such wireless networks are termed as rogue WLANs. Rogue WLANs can therefore be access points, laptops deployed as access points, user stations, barcode scanners and printers. The rogue access points and even the wireless laptops are supposed to configure with at least basic wireless security standards. The improperly configured WLANS can originate network vulnerabilities. Improper configuration includes deploying wireless network in an area where there is already another wireless network. There is possibility to access wireless network by people in another wireless network under if the APs are misconfigured. Therefore, the position of the access point should be marked to avoid collision with neighboring network. The rogue access points and some other vulnerabilities can be detected through freeware like NetStumber and Kismet. Since, the rogue access point and /or WLAN may get created any time, it requires periodic checking through such freeware. For best results, constant monitoring almost everyday is to be performed. It helps in obtaining the precise information about hacks and attacks.

Separate set of wireless intrusion detection sensors can be effective wireless security technique to mitigate attacks in wireless network.

2. **Lock Down all Access Points and Devices:** This security technique involves configuring the APs and wireless stations like laptops so as to control the unwanted connections. The user stations should be installed with software that ensures that security policies are being deployed. The software should alert the users in case any security breaches are made. Likewise, enterprise-class access points are to be considered to enhance the wireless security. The enterprise-class access points are embedded with advance security policies. The common mistake that paves easy path for intruders is selecting the default Service Set Identifier (SSID). SSID is the name of the AP. The default SSID names are predictable. Therefore, the network administrators should change the SSID name with something unpredictable names. This makes tough for the intruders to coin the name of the SSID, preventing them to recognize the APs. More security can be achieved if the broadcasting mode of SSID is disabled. Thus, the network users need to know the SSID before making connection requests. The enterprise-class APs has feature of filtering connections based on MAC address. Likewise, a policy with disabling the slower connection, disables the connection attempt from outside of the targeted WLAN periphery.

3. **Encryption and Authentication:** Encryption and authentication are key elements for wireless security. However, there exist no completely reliable encryption and authentication techniques. Just one can do is to select the most efficient tools and secure the WLAN as far as possible. The 802.11 standard based protocols, especially WEP has been proved unsecured as encrypted traffic can be easily decrypted. Even the hackers have created tools that decrypt the traffic encrypted by the WEP protocol. Therefore, security conscious network administrators are focusing on VPN for enhanced encryption and authentication between APs and the network clients. Likewise, radius server has been considered for securely managing authentication, accounting and access to the network resources.

4. **Set and Force WLAN Policies:** The security policies requirements in WLANs may vary from enterprise to enterprise. Each enterprise defines its own set of security policies based on their needs and concerns. Whatever are the needs, the security policies should prevent from unauthorized access to the access points at first. Access points are where WEP or VPN connections are implemented. Similarly, SSID is also associated with access point. Therefore, proper security policies should be developed for access points. Also, reconfiguration of access points and WLAN cards should be restricted to prevent from making changes to predefined configurations in APs.

   Another security policy generally implemented in securing WLAN is setting channel speed and connection time. Normally, the connection

speed of the channel is set up to be 5.5 Mb/s or 11 Mb/s. Any connection not following the prescribed channel speed, are considered as malicious connection and thus terminated. To ensure that the intruders not try to connect during the office off hours, time policy can be made. Any connection attempts other than during the stated time in the security policy, are again considered as malicious connection attempts and thus terminated, regardless of users even they are the office staffs. The policy enforcement is equally important as the policy itself. In addition, the policies should monitor the security vulnerabilities as much as possible. The most effective would be monitoring every moment as far as possible.

5. **Intrusion Detection and Prevention:** Proper intrusion detection and prevention system tools can contribute in security system in wireless network effectively and efficiently. Intrusion prevention system (IDS) restricts the malicious traffic from reaching the internal network or at least sensitive area of the network. Intrusion detection and prevention system are supposed to monitor every traffic coming inside the network and assure that they are totally harmless. Every day hackers are trying with new approaches of hacking and attacking the WLAN. Hence, security policies should be well defined in IDS, and should be adaptable to recognize the emerging threats in the WLAN.

2.3.3 Security Threats in Wireless Local Area Network

Wireless network has been targeted network for hackers and attackers. The reason behind is ease of intrusion and availability of wide vulnerable areas in wireless networks. Therefore, to assure security, developer and implementer of WLAN should have idea about various possible threats that are likely to be encountered in the WLAN. Previously, wireless devices were costly and thus attacks were minimum but today, most devices have wireless service therefore, attacks in WLAN have significantly burst up. The following attacks are common on wireless networks [15]:

Denial of Service Attack

Denial of Service Attack (DoS Attack) floods the traffic in networks preventing the legitimate users accessing the network resources. DoS attacks can even be unintended but may have severe effects, particularly for low capacity data flow network. The DoS attack differs between wired and wireless network only at network, data-link and physical layer. At network layer level, DoS attack is common as IEEE 802.11 wireless standard is a shared medium. Thus, malicious users can find an easy path to flood the network. Such simple and common DoS attack can be flooding the gateway with Internet Control Message Protocol (ICMP) message. 802.11b easily gets saturated, thus it is prone to DoS attack.

In data-link layer, the same easy access to the medium makes it easy for attackers to come up with DoS Attack. Despite the WEP security, the intruders can access the link layer information. With no WEP security

implemented, the client is always open to DoS attacks from the spoofed APs. At physical layer, the attacker can create the similar frequency bands as used by 802.11 wireless standard. Thus, they can easily saturate the channels with introducing noises. There exists many devices that generate the signals operate at 2.4 GHz. These devices can easily make WLAN down. For examples, cordless devices use the same frequency as that of 802.11b and Bluetooth devices use the frequency band as used by 802.11b and 802.11g. Thus, it paves easy path for the attackers to produce interference in the wireless channels; curbing users of the network unable to access the desired data.

Man-in-the-Middle Attack

Two forms of Man in the Middle Attacks are found in WLAN, eavesdropping and manipulation. Eavesdropping is simply recording and analyzing the traffic flowing in the network while manipulation means accessing the traffic, making changes and re-transmitting the altered data back to network.

1. **Eavesdropping**: Since the radio signals are omnipresent inside the specific range, there is every possibility for an attacker to access and even store the traffic flowing in the wireless network. Although, the transmission of signals are supposed to deteriorate after certain distance, with efficient wireless antenna, one can access the wireless signals over much longer distance, even from miles away. The only way to prevent useful network information from eavesdropping is the deployment of efficient encryption techniques. So; the developers of WLAN have introduced WEP security. But, WEP in itself has many flaws. Thus, it cannot prevent network information from eavesdropping. This seeks more security policies implementation requirements at higher levels. They can be IPsec, SSH or SSL (Secured Socket Layer) security policies. Another idea behind preventing eavesdropping is to stop unauthorized access of the network traffic from the third parties. Noureddine [15] suggests the following techniques to tackle with eavesdropping:

    a. the antenna positioning and shielding use
    b. the control of the use of a particular antenna, when the device supports antenna diversity
    c. the control of transmitted signal strength
    d. the use of directional antennas and use of shielding points

2. **Manipulation**: Manipulation is the further further extended violence of eavesdropping. The attacker who assesses the network traffic can alter the network traffic and resend the changed traffic. The attackers can introduce rogue AP in the wireless network. It is a spoofed Wireless Access Point (AP). As wireless devices are made to join the most powerful APs, the victim may join such rogue APs, whereby the attackers can record the victims data, analyze them, alter them

with wrong data or even block the data flowing to the victims. Under no security policies or low level of security policies, the attackers can easily determine the SSID associated with the wireless network and can make easy entry in such network. WEP is supposed to obscure such unwanted intrusion from third parties. But, as it is found not less effective, the manipulation can be controlled with authentication, authorization and accounting of the users connecting to the wireless network.

Message Modification and Injection

It has been proved that traffic encrypted by WEP can be altered in the during transmission. The attackers involved here takes advantage of linearity function used by the WEP checksum. The attackers can alter the original message without altering the checksum and without accessing the traffic physically. They can just alter data mid-way. The task needed for the attackers is to maintain the same checksum before and after such alterations. Since checksum is the unkeyed function of messages and WEP does not prevent secure access control, the adversary can compute the checksums after having knowledge of the message. As the attacker can get familiarized with the entire messages of any transmitted frame, he can inject some arbitrary data without bringing changes in the checksum of the frame.

Message Decryption

As the attackers can manipulate the encrypted traffic without detection in WLANs, they can even decrypt the traffics flowing. For this purpose, the attackers can target on APs. They can misuse the AP address and decrypt the cipher text in the following two ways:

1. **IP Redirection**: IP redirection is to sniff the encrypted packets and then spoof IP address of the APs that is changing the destination IP address of the packets being delivered in the WLAN. However, it requires the APs to function as router for internet connectivity in the network. WEP is all about granting permission to access the WLAN. Thus, WEP opens path for accessing the APs. The APs can then be directed to decrypt the traffic and alter the destination address. This leads the traffic to flow from the WLAN to the attackers residing in the internet network. The challenge for the attackers here are to coin out the destination IP address and assuring the checksum of the traffic is still the same after altering the destination address. The formal task is relatively straight-forward. It is easy to find out the IP address of the subnet being used by the WLAN. With decryption of such traffic flowing to such network, one can find out the IP address of the other side taking part in communication. Thus, one can find out the destination IP address and thus makes it possible to change it. But, attackers need to come up with more efforts maintaining the checksum. If the checksum is previously known, attackers just need some simple XORing the previous and new checksum and find the value for the

value of the IP to be changed to maintain the same checksum. But if the checksum is not exposed in advance, the attackers require going with hit and trial method for finding checksum.

2. **Reaction Attack**: In any TCP/IP traffic, the recipient confirms the validity of the incoming packet with acknowledgement in response if the packet passes checksum check. And WEP might be used to secure TCP/IP traffic. Under these two conditions, attackers can make reaction attacks. Thus, the reaction attack is based on acknowledgement packet sent by the receivers. The acknowledgement packets can simply be tracked, as these packets are relatively smaller avoiding the need of decryption. The attackers start with flipping few bits in the cipher-text adjusting the encrypted CRC accordingly to get a new cipher-text. Then, the packet is injected in the network to see if it passes the checksum or not that is if it responds with acknowledgment or not. The presence or the absence of the TCP acknowledgment, provides a bit information of the packet. The attackers continues altering the position of the flipped bits and eventually, the whole packet information can be retrieved.

2.3.4 Wireless Security Protocols

The earlier thinking behind the development of wireless network was to provide the end users with easy access to the network. The developers came up with their objectives behind. But, with the provision of easy access to such wireless network, the inherent threats also came into existence and adverse effect went on boosting because of unwanted accesses. To combat such unwanted accesses and the possible threats; the developers of wireless security have introduced several security protocols. The basic idea behind such security protocols is found to meet the wire equivalent security in the wireless network. Even the first security protocols developed for wireless network is Wire Equivalent Privacy (WEP). Other security protocols are Wifi Protected Access (WPA) and Temporal Key Integrity Protocol (TKIP). Nowadays, these wireless security protocols are embedded with wireless devices like routers and other access points. Details on these wireless security protocols are discussed below.

Wired Equivalent Privacy (WEP)

WEP is first wireless security protocol that came into existence to control wireless threats [18, 19]. The idea behind was to facilitate the wireless network with wired level security. The task is completed via encryption technique through RC4 algorithm at both sender side and receiver side during the data communication [20]. RC4 is the most popular stream cipher in the world of cryptography that provides a pseudo random stream of bits. RC4 prevents from the hackers attempt to [18, 21, 19]. WEP implements the combination of secret key and encryption to secure traffic. The secret key consists of a simple password of either 5 characters or 8 characters [18]. This secret key is of 40 bits with 24 Initialization Vector (IV). Without the

IV, the security key would generate the same cipher-text. Thus, with use of IV, each time different cipher-text is generated. This prevents attackers from eavesdropping the data pattern [20]. The augmented key acts as both encryption and decryption keys [20].

At the sender side, the user data (plain-text) is passed through Integrity Check (IC) and the checksum is calculated. This checksum is appended with the user data through exclusive-or (XOR) function [20]. The concatenated stream is then encrypted with the shared key through RC4 algorithm. Such encrypted data are the final data to be transmitted in the network along with IV. At the receiver end, at first, the secret key is generated from shared key and IV provided along with cipher text. This secret key decrypts the cipher text and produces plaint text and IC checksum. The plaint text again goes through IC and generates new IC checksum. Finally, the old and the new IC checksums are compared to assure the data integrity

WEP Security Weaknesses With references to the articles "A Survey on Wireless Security Protocols (WEP, WPA and WPA2(802.11i)" [20] and "Choosing the Right Wireless LAN Security Protocol for the Home and Business User" [20], the following security problems are associated with WEP protocol.

- WEP is unable to control packet forgery and replay attacks.
- WEP uses RC4 algorithm, which has flaws in itself, and further the algorithm is improperly utilized. The secret keys considered are weak enough so that they can be easily brute-forced with open software.
- WEP encrypted cipher-text that can easily be decrypted without having the need to know the security keys. Even no smooth updates are available for security keys.

Wifi Protected Access (WPA)

WPA came into existence so as to overcome the shortcomings of the WEP cryptography protocol. WPA has two operation modes [20]:

- **Personal WPA or WPA-PSK (Pre-Shared Key):** This type of cryptography method is intended for home or small business organization. The protocol does not use authentication server. The cryptography key implemented can be alphanumeric and range up to 256 bits. This key is prevented from transferring in the network. Both the AP and station are provided with such cryptography key. In this way, WPA facilitates the mutual authentication. The WPA key is deployed only initiate initial session with APs.
- **Enterprise WPA or Commercial WPA or WPA-TKIP:** Enterprise WPA implements 802.1X+EAP during authentication procedure. 802.1X+EAP (Extensible Authentication Protocol) is an authentication protocol developed for IEEE 802 (wireless) networks.

It assists in transferring authentication messages between wireless users and authentication server, thereby, eliminating the burden of authentication task from APs. Likewise, WPA-TKIP implements more advanced TKIP encryption. The enhanced protocol obviates the use of preshared key during authentication. But, it requires Remote Authentication Dial-In User Service (RADIUS) server for authentication mechanism [18, 20, 22].

- **Wifi Protected Access 2 (WPA2):** WPA2 implements the Advanced Encryption Standard (AES) for security purpose. AES is the government standard security [22]. It is operable in both personal and enterprise level and has been found most effective in to combat entry of intrusions in the wireless network [18, 20, 22].

2.4 Wireless Body Area Network

Wireless Body Area Network (WBAN) often referred to as WPAN; is a network of sensor nodes are configured on or inside the human body. The data collected by these sensors are retrieved by personal devices like PDAs, smart-phones, tablets etc [23]. The WBAN has evolved as the possible solution to technical challenge associated with real-time health monitoring system. In health sector, the technology has been used to alert both doctors and patients about the health problems or progress of the patient in real-time. Besides, the WBAN technology is also deployed in non-medical sector like sports, video streaming, date file transfer and so on [24]. IEEE Task Group 6 (TG) have developed the wireless standard 802.15.6 for the WBAN. The concentration has been made on lower power consumption device. This is because these devices are intended for transferring the critical medical data to remote receivers. The devices should operate for longer time, consuming significantly lower power [24, 6, 25, 26, 27, 23, 28]. Through the implementation of body sensors, the pervasive technology can be deployed in the WBAN to accomplish the task of remote medical services in health sector [27]. Figure 2.3 depicts the simple deployment of the WBAN along with constituent equipment those are implemented in the WBAN.

2.4.1 WBAN Security Issues

Since the nodes in the WBAN are intended to transfer vital and critical patient data, various concerns are emerged during the technology design. Bandwidth selection, channel modeling, MAC protocol design, energy-efficient hardware, reliability and availability, security and privacy are some of the important issues which are considered during technology design [24]. The security issues in the WBAN are summarized below [24]:

- **Data Confidentiality:** As the nodes in the WBAN have their role in transferring the critical patient data, the WBAN should be able to hold data confidentiality. Patients data should be prevented from disclosing among non-concerned people or network.

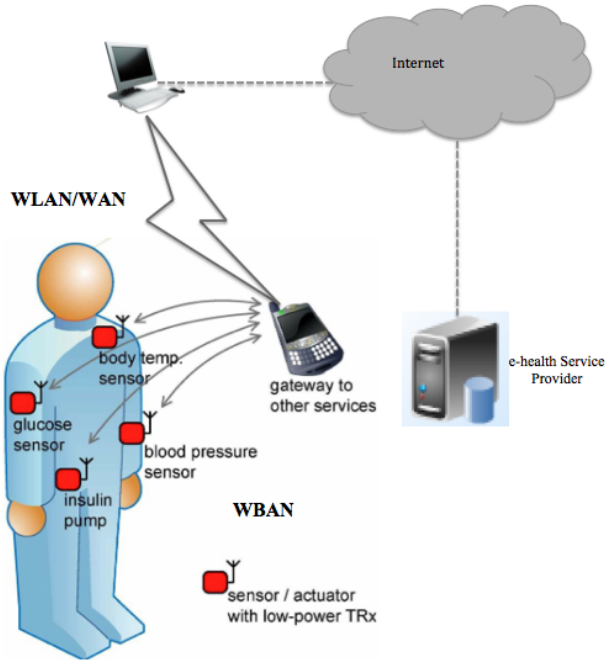


Figure 2.3: *Simple deployment of the WBAN network with it's network components*

- **Data Integrity:** Data integrity bears no meaning unless data are prevented from alterations. Since in the wireless network, data alteration in the mid way by intruders has become common attack, data integrity should be effectively handled in the WBAN. The data integrity often occurs as a result of data loss during transmission. Thus, even the physical channels are supposed to absolutely reliable.
- **Data Authentication:** Often the intruders may come up with fabricated data in the WBAN. Under this condition, the WBAN should be facilitated with the ability to authenticate the original source of the data.
- **Secure Localization:** Sometimes, finding out the exact location of the patients become very important to prevent unwanted accidents. Nevertheless there is every possibility that intruders may alter the location of the patient. Thus, the WBAN implementation should also consider this issue.
- **Availability:** As previously mentioned, devices in the WBAN are supposed to be up for ever or at least efficient back-up devices should be deployed. However, due to easy availability nature of wireless network, the intruder might be able to obstruct the operation of the nodes. Interruption in transmission of critical data are absolutely undesirable in the such network.

The security issues discussed above are summarized and presented in Table 2.2 with possible solutions:

Table 2.2: *Summary of security issues in the WBAN with possible solutions*

Security Issues	Threats	Possible Solutions
Data confidentiality	Message disclosure	Link/Network Layer encryption, access control
Data integrity	Message Modification	Keyed secure hash function, digital signature
Data authentication	Unauthenticated/ unauthorized access	Random key distribution public key cryptography
Secure localization	False patient location	Smart tracking
Availability	DoS attacks	Intrusion detection, redundancy

2.4.2 Threats in WBAN

Still the WBAN technology is in the nascent stage. It requires lots of further research for assuring higher degree of reliability and are being conducted too. There exists several security challenges in the WBAN as the standard is quite different from the existing wireless standards. Further, data traffic under consideration in the WBAN is comparatively critical than other wireless networks [23]. One of the major challenges for the WBAN is undeterred availability of network devices and channels. To achieve such availability of network resources, DoS attacks should be completely eliminated from the network. The threats in the WBAN can generalized as privacy violation and physical attack [24]. In this thesis, different types of DoS attacks and their possible solutions are presented on layered basis. Figure 2.4 below presents quick overview of the DoS attacks with brief overview [24, 25]:

2.4.3 WBAN Security Model

In order to maintain the expected security in the WBAN, 802.15.4 has defined three levels of security [28]. With increase in level numbers, the security level also increases. The three security levels are presented below:

- **Level 0:** The level 0 provides no security at all. It is an unsecured communication. There exists no provisions of data authentication and integrity. Plus, it provides no confidentiality and privacy. Also, it is unable to handle replay attacks.

- **Level 1:** This is the medium level of security that the standard provides in the WBAN. It provides the facility of authentication prior to data transfer, but it still lacks data encryption. This security level also fails against confidentiality and replay attacks.

- **Level 2:** This is the most advance security level that the WBAN standard has designed. The data communication takes place under secured authentication and with encryption. This security level also provides the solution to confidentiality need and replay attacks.

Layers	DoS Attacks	Preventions
Physical Layer	Jamming	Spread-spectrum priority messages, lower cycle, region mapping, mode change
	Tampering	Tamper-proof, hiding
Data Link Layer	Collision	Error-correcting code
	Unfairness	Small frames
	Exhaustion	Rate limitation
Network Layer	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization monitoring
	Black holes	Authorization, Monitoring, redundancy
Transport Layer	Flooding	Client puzzles
	De-synchronization	Authentication

Figure 2.4: *Layered presentation of DoS security threats with preventive measures*

2.5 ZigBee Network

ZigBee network extends the 802.15.4 standard to Network Layer of OSI model that is ZigBee works on the top of 802.15.4 standard [29]. Precisely, ZigBee enhances 802.15.4 standard providing Network Layer with security and Application Layer [29, 30]. This enhancement provides ZigBee standard broad application area. The standard has been deployed in different automation process, telecom services, health care system, smart energy system and lots more [29]. 802.15.4 is unable to support multi-hop networking and mesh networking [31]. This shortcoming is eradicated by ZigBee and can provide a single network platform to communicate more than 64000 devices [29]. Figure 2.5 provides vision of layered architecture of the ZigBee network. 802.15.4 operates at lower two layers denoted by with pink block and ZigBee operates on the upper two layers as denoted by yellow-green color. These devices can be connected in Mesh Topology, Star Topology or Tree Topology [29, 30]. ZigBee is thus designed to communicated largest number of devices through single platform [29].

Figure 2.6 represents a simple ZigBee network with different ZigBee network components. ZigBee has two versions: ZigBee 2006 and ZigBee PRO [2]. ZigBee PRO is the advanced version of ZigBee 2006.

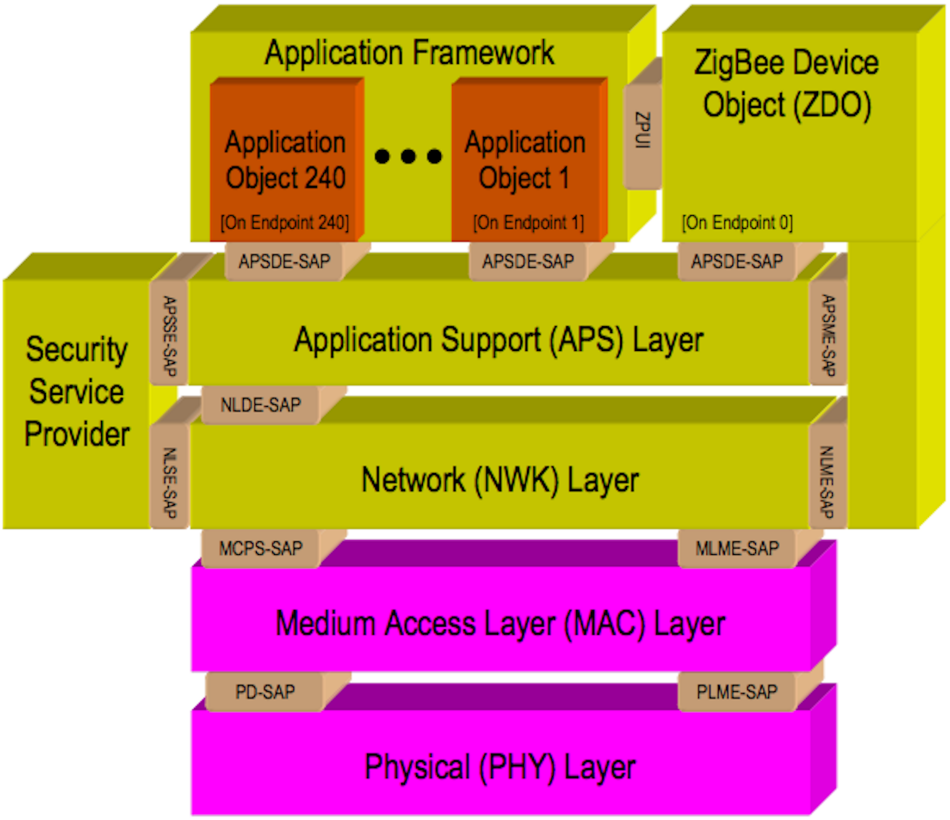


Figure 2.5: *Layered presentation of ZigBee network [2]*

- **ZigBee Coordinator:** Coordinator is the pivot of a ZigBee network. It is responsible for managing and securing the network [29]. Single Coordinator is enough to manage a ZigBee network. It provides channel number and PAN id to other devices [31].
- **ZigBee Router:** Router serves as platform for communicating end devices with the Coordinator. Routers in ZigBee network are optional, but used it builds Neighbor Table as a database of Neighbor Routing [31].
- **ZigBee End Device:** End Devices are also optional in ZigBee Network [31]. The activities of these devices are primarily governed by the Coordinator. End devices collect data that they sense and relay to the Coordinator. These devices go to sleep mode when no data communication take place to preserve energy [31].

Figure 2.6 shows a network formed by using a Coordinator, four Routers and two End Devices.

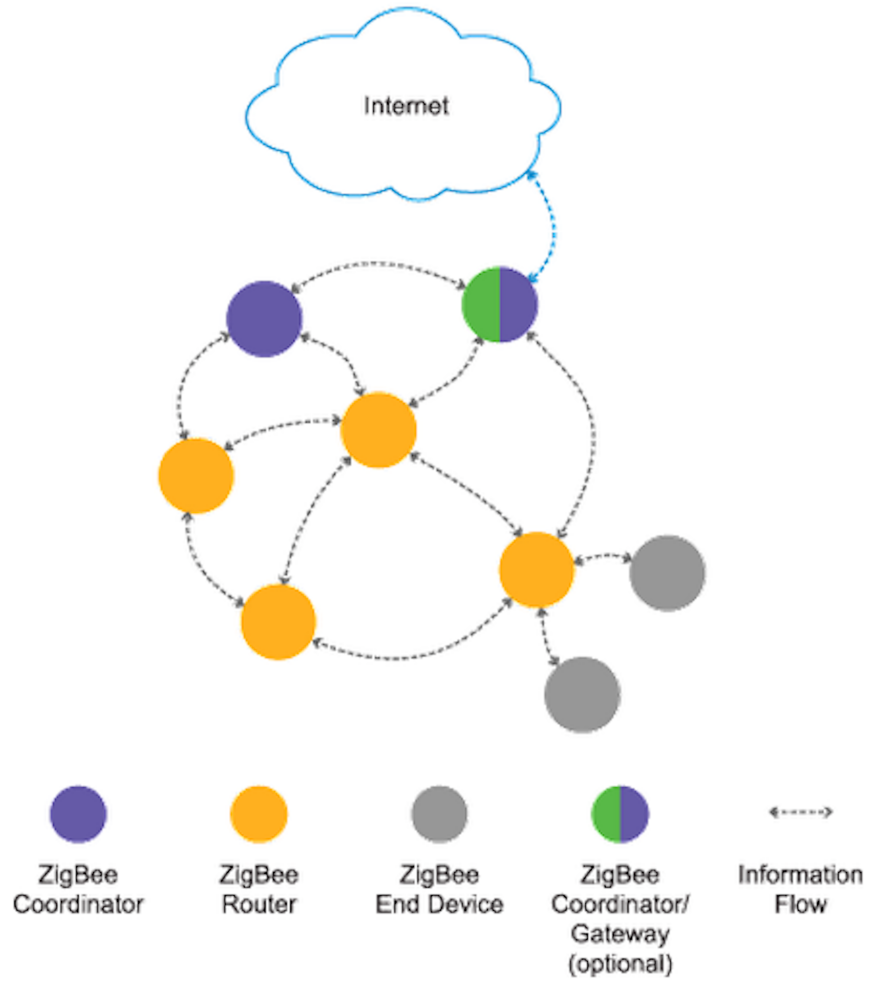


Figure 2.6: *A simple ZigBee network with different components*

Data communication in ZigBee network takes place in 27 channels [29, 31]. These channels are divided for three different frequency bands 868 MHz, 915 MHz and 2.4 GHz [29, 32]. Table 2.3 provides the overview of channels division based on frequency band.

Table 2.3: *Distribution of channels in physical layer*

Frequency Band	Bit Rate	Channels	Geographical Area
868 MHz	20 kbps	1	Europe
915 MHz	40 kbps	10	EEUU
2.4 GHz	250 kbps	16	Worldwide

2.5.1 Features

The following features are associated with ZigBee specification that places it on the top of other sensor networks [2]:

- Lower power consumption
- Comparatively cheaper
- More reliable and faster
- Huge node network with easy deployment
- More secure with network layer security
- Globally deployable and inter-operable

2.5.2 ZigBee Network Management

In ZigBee network, devices can join the network through two procedures: MAC Association and NWK rejoin [2]. The two methods are discussed below.

MAC Association

MAC Association is mandatory procedure for joining a ZigBee network [2]. Figure 2.7 provides a pictorial view of MAC Association. The device (mainly Coordinator) that wants other device to participate in the network; sends *NLME-PERMIT-JOINING request*. The joining devices discovers the network to join based on the request command issued by the previous device. The discovery of network is accomplished through *Beacon request* command. The end devices then issue *NLME-JOIN request* with *Association request* command. MAC Association technique to join network is completed with *Association response* command. MAC addresses are recorded during *MAC Association request/response*. MAC Association does not have any security system. All the frames during MAC Association are transmitted in plain text [2].

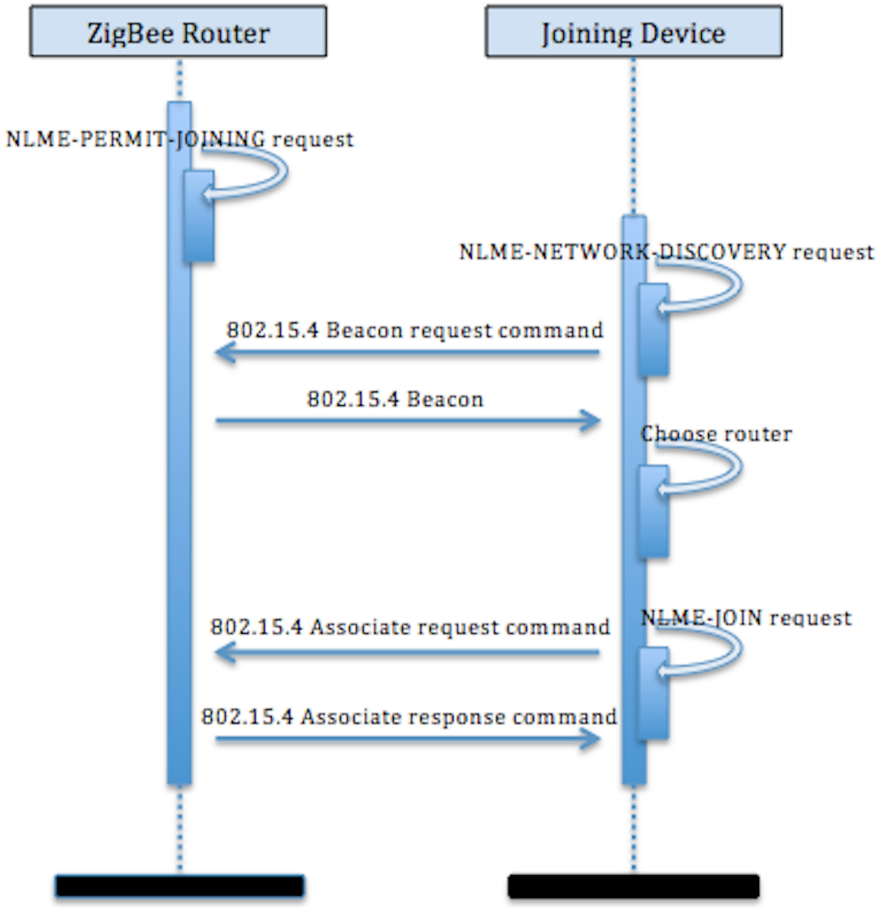


Figure 2.7: *Network joining procedure with MAC Association protocol [2]*

NWK Rejoin

This is secure way of joining a ZigBee network [2]. Figure 2.8 provides a vision of network joining procedures undertaken by NWK Rejoin protocol. The communication is encrypted with NWK Key that is previously provided by the Coordinator. If the device is joining for the first time, there should be some provision of transferring NWK Key to joining devices [2]. With this protocol, joining devices need not wait for *NLME JOINING request* from upper device. They initiate network joining procedure by issuing *NLME-JOIN request* via *NWK Rejoin request* command [2].

2.5.3 Security Techniques in ZigBee

ZigBee is developed as more secure the WBAN deployment than traditional 802.15.4 network. In addition to security system maintained by Physical Layer and Data-link Layer of 802.15.4 network, it provides the security at Network Layer and Transport Layer [29, 32, 2]. The extended security system is grounded on 128-bit AES encryption [2]. The security system in ZigBee is meant for securing key management, device management and frame protection [2]. Security is organized in three layers viz, MAC Layer,

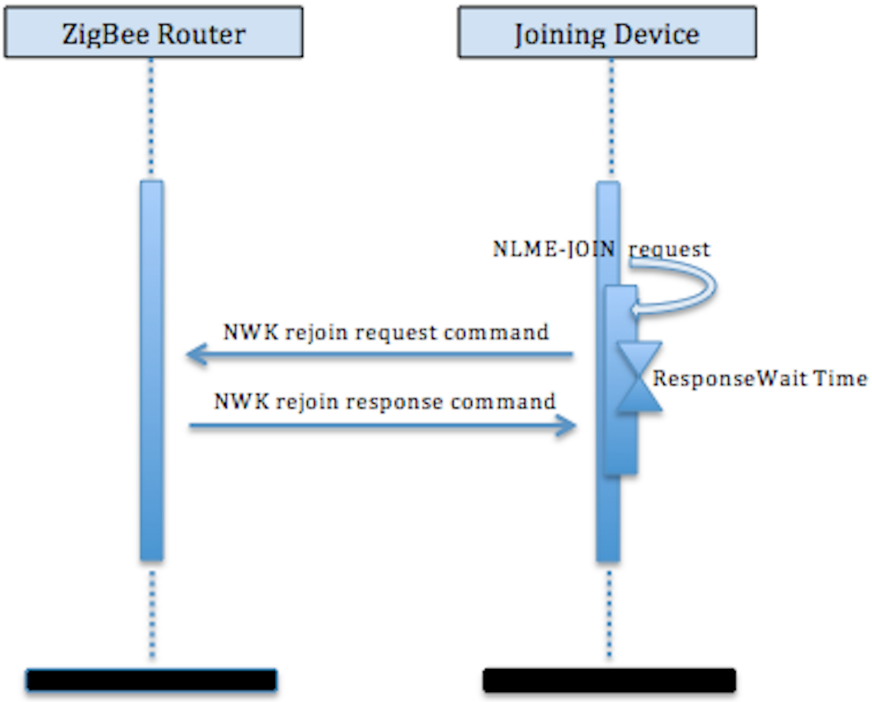


Figure 2.8: *Network joining procedure with NWK Rejoin protocol [2]*

Network (NWK) Layer and Application (APS) Layer. Security system in ZigBee can be classified into two parts [2]:

- Trust Center
- Security Keys

Trust Center

Trust center is usually a Coordinator, but it can be any other dedicated device. Trust center manages network devices. It decides whether to permit or deny the End Devices to join the network. It also updates the network key periodically. The role of such trust center can be further divided into three as [2]:

- **Trust Manager:** Authenticate End Devices willing to join network
- **Network Manager:** Manage network keys
- **Configuration Manager:** Assure end-to-end security among devices

Security Keys:

In order to maintain security, ZigBee implements three types of keys [2]:

- Master Keys: Master Keys are used to encrypt Link Keys establishment procedure that are actually used for frame encryption. They can

be Trust Center Master Keys generated by Trust Center or Application Layer Master Keys.

- Network Keys: These keys encrypt the Network Layer communication and there exist only one Network Key at a time for every End Devices.

- Link Keys: Link Keys encrypts only unicast messages flowing between End Devices at Application Layer. It can be either Trust Center Link Key or Application Link Key.

2.5.4 Security Mode

ZigBee PRO provides two types of security modes: Standard Security Mode and High Security Mode [2]. Standard Security Mode is fairly simpler and thus consumes less RAM than that of High Security Mode [2]. The features of each mode is mentioned in Table 2.4.

Table 2.4: *Security Mode [2]*

Feature	Standard	High
Network Layer security provided using a Network Key	yes	yes
APS Layer security provided using Link Keys	yes	yes
Centralized control and update of keys	yes	yes
Ability to switch from active to secondary keys	yes	yes
Ability to derive link keys between devices	no	yes
Entity authentication and permissions table support	no	yes

2.6 Intrusion Detection and Prevention System

Whatever the dictionary meaning of intrusion has, in computing security, it refers to an attempt that may render a computer system down or accessing unauthorized traffic or manipulating the information from such traffic. Such attempts need not necessarily be successful. Even the unsuccessful attempts are counted as intrusions for they are against security policies. Thus, it is good idea to keep track of both successful and unsuccessful attempts of intruding in the computer network. This helps to get knowledge of what sort of traffic is flowing in a computer network and eventually assists in designing more secure security policies. Usually, security professionals place traffic monitoring devices; termed as sensors, in front (unsecured area) or behind the firewall (secured area). Thereby, the traffic flowing in both sides of the firewall are compared and analyzed. The preventive methods used for deterring the malicious traffic, have generally three disadvantages. First, preventive methods are unable to filter out certain wormhole and sinkhole, second, they require large processing and storage, and finally, as wireless network is affected by varieties of attacks, no single prevention method is found efficient [33]. However, it does not mean to deploy multiple prevention systems in a single network.

2.6.1 Intrusion Detection Mechanisms

Different types of intrusion detection system are found in the network security. Differentiation is made based on the techniques, such tools identify the intrusions. In general, intrusion detection system is classified into two groups:

Signature/Rule Based Detection

Signature based intrusion detection system implements signatures stored to identify the attacks based on the database of well-known attacks. This type of intrusion detection system consists of three stages. First, data acquisition phase where the nodes monitor and collect the required data from the network traffic for inspection. Second, rule application phase where the data considered for analysis are fetched by application rules. Finally, intrusion detection phase where alert signals are created based on abnormal data pattern from that of normal data pattern [34]. Thus, such intrusion detection tools have limited scope as new attacks are emerging day by day in computer networks. The database of known attacks needs to be updated frequently.

Anomaly Based Detection

In anomaly based detection method, a model is prepared for the normal and expected traffic. Any traffic that does not follow the pattern of normal traffic; are considered as anomaly. And thus, they are differentiated as attacks or intrusions [35]. As anomaly based intrusion detection has potentiality to coin out new attacks, they are preferred over signature based intrusion detection system. This type of detection system has ability to filter out new unknown threats, but at the same time, it is susceptible to higher false positives. Anomaly based detection system is further classified into three groups, namely:

- Supervised
- Semisupervised
- Unsupervised

Figure 2.9 presents the diagrammatic presentation of different types of intrusion detection mechanisms with quick overview.

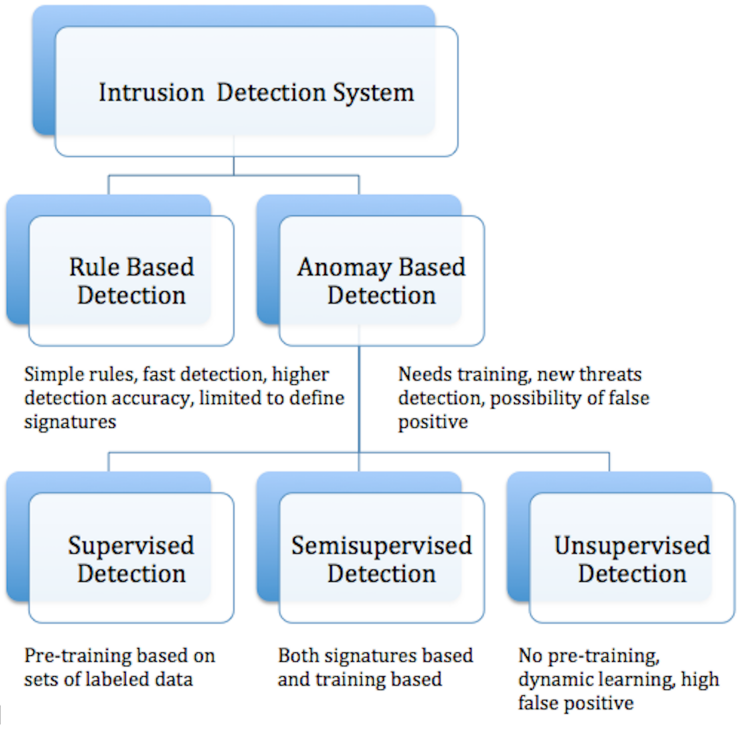


Figure 2.9: *Classification of intrusion detection mechanisms*

2.6.2 Intrusion Detection System (IDS)

Intrusions are malicious actions that tend to bypass the security system of network systems. These actions attempt to break through integrity, availability or confidentiality of computer a network resource. The definition of Intrusion Detection System is found inconsistent. The definition differs with different security researchers and experts. In a book named Intrusion Detection & Prevention, Endorf, Schulz and Mellander define intrusion detection system as a tool, a method or a system of resources with ability to identify, assess and report unauthorized or unapproved network activity. Such IDS do not detect intrusions by themselves. They detect the activities being performed on network traffic, and not necessarily be intrusions. Intrusion detection constitutes a part of the overall protection system, installed in a device or a system.

One can make analogy of a computer protection system with that of private house with valuable assets in it [19]. The locked doors act as firewalls, security alarm as IDS and guard dogs as Intrusion Prevention System (IPS). The locked doors prevent authorized access in the building. They do not alert about people knocking at the door. But, in case they enter the door, security alarm alerts about their entry and thus, the possible threats that may undertake. The guard dogs then, have their role in trying to prevent the intruders run away and prevent the possible harms. Likewise, the firewall just tries to drop the harmful traffics based on the policies defined for it. The IDS alerts about intruders and IPS deploys the prevention policies to nullify the possible threats from such intruders. Precisely, IDS is just a part

of security system. All these three components complement each other to contribute as a security system.

The effectiveness and efficiency of security system are based on the deployment of firewall, IDS and IPS. For example, the house will be more secured if all the doors and windows are locked, security alarms are installed in every doors and windows and many guard dogs are deployed. Similarly, it is wise from security point of view to install firewalls, IDS and IPS at every entry point to enhance the overall security system. Intrusion detection consists of three steps [36]:

- Monitoring the network traffic and then analyzing
- Identifying the anomalous activities
- Assessing severity and generating alerts

2.6.3 Types of Intrusion Detection System

The intrusion detection and prevention system operates in layer three; the network layer of the layered architecture. Like in antivirus, a set of alert signatures are defined for the IDS, and they generate alerts based on those set of rules defined to point out the malicious activities, undertaking in the network. Such unwanted malicious activities need not always be harmful. The unwanted activities may occur as misuse of system or network equipment. In this regard, intrusion detection system can roughly divided into two types: Misuse Detection and Anomaly Detection [33]. Misuse Detection simply alerts about unwanted traffics in the network, based on provided threat signatures. On the other hand, Anomaly Detection generates alarm if the network traffic is found deviated from the normal network traffic. The Anomaly Detection method are developed with ability to learn from normal traffic and thus, are embedded with adaptive threats detection capability. Further, intense study has been carried out for better improvement of adaptability [33]. Different IDS have different threats detection methods. The benefits of deploying IDS depend upon the detection method chosen. An IDS can be knowledge-based, behavior-based, stand alone or the combination of all. The knowledge-based IDSes generate alert messages before any intrusion takes place, based on database of common threats. Likewise, the behavior-based IDSes generate alerts tracking the expected use of the resources by traffic. The stand alone IDSes operate at background passively, monitoring and logging the network traffic and logging the alerts in case any suspicious actions are being monitored. The choice of organizational need of intrusion detection system is based on their requirements.

Currently, three types of intrusion detection systems are under implementation:

i Host-Based Intrusion Detection System (HIDS)

ii Network-Based Intrusion Detection System (NIDS)

iii Hybrid Intrusion Detection System

Host-Based Intrusion Detection System (HIDS)

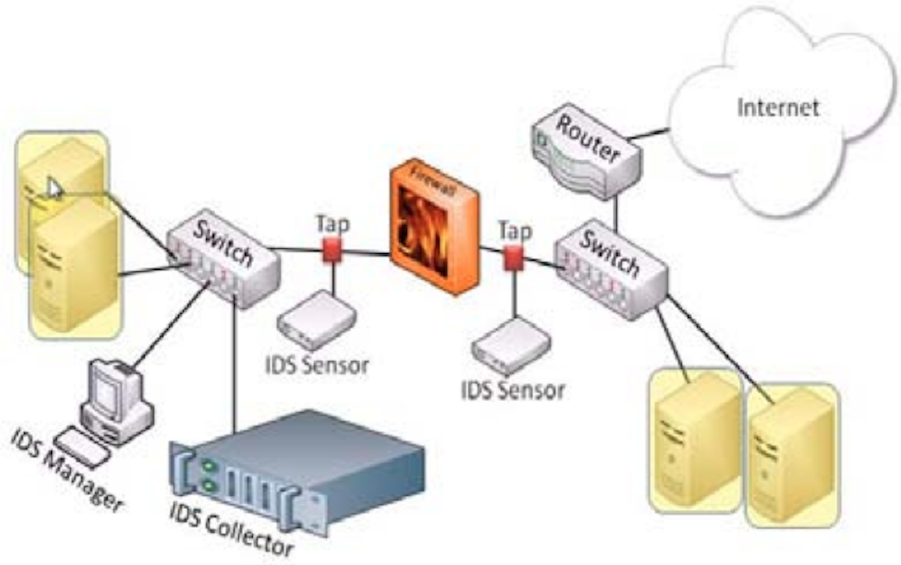


Figure 2.10: *Sample Host Based Intrusion Detection System, IDS agent is installed in each computers as highlighted*

HIDS consists of software installed in a host computer that examines all the activities undertaking in the computer network. It scans the computer resources and associated traffic. The idea is to implement the detection system in all host computers. As the intrusion detection tool is installed in every hosts, it ensures the efficient intrusion detection system. Figure 2.10 shows a general overview of a HIDS deployment. IDSes operation is based on different log files such as kernel log files, system log files, firewall log files, network log files and more. IDSes compare these log files against the database of threat signatures [37]. Thus, a HIDS analyses different computer system log files, makes analysis and compares with the known signatures for threat recognition and creates own log files for the security analyst. IDS may also check the data integrity of the files. It generates the checksum of each file under consideration with message-file digest technique such as md5sum or sha1sum [37]. These checksums are stored in a plain-text file and compares the original files periodically to ensure the checksum integrity with that of values stored in the plain text files. Tripwire SWATCH (Simple Watcher), LIDS (Linux Intrusion Detection System) and RPM (Red-Hat Packet Manager) Packet Manager are some examples of such host based intrusion detection for Linux platform.

Network-Based Intrusion Detection System(NIDS)

NIDS has different philosophy in comparison with HIDS. It monitors and analyses the network traffic either at router level or host level [37]. Then, the packet information monitoring task is audited and logged to new file with

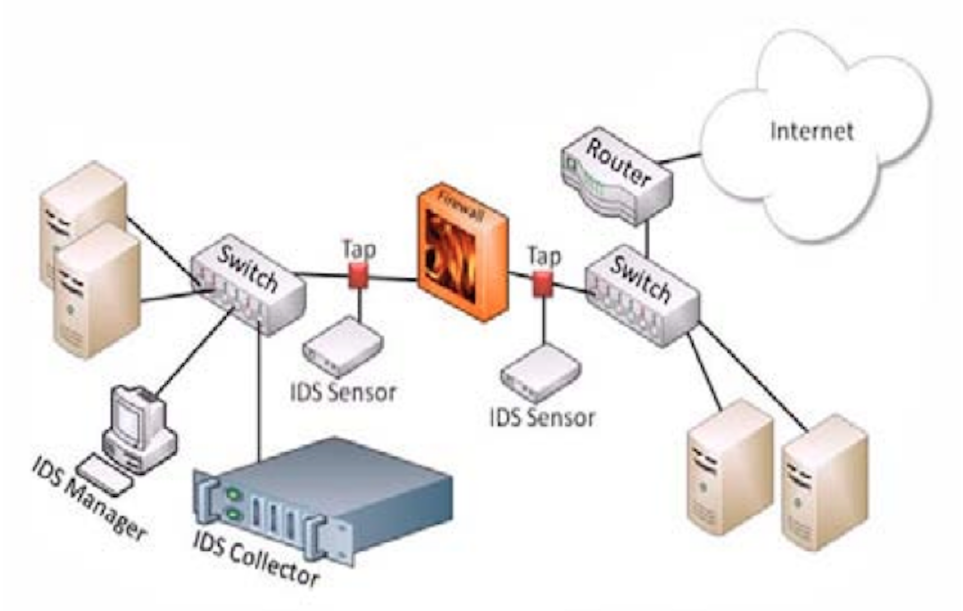


Figure 2.11: *Sample Network Based Intrusion Detection System*

additional information in case any doubtful traffic are found. NIDS then, compares such doubtful behavior with predefined threat signature database. Finally, security messages are generated to alert the security professionals about probable intrusions in the network. Figure 2.11 provides a general overview of an NID deployment. NIDS has its significance in large network, specially, internet where voluminous traffic flows each second. Thus, NIDS is expected to be able to monitor such large traffic and successfully coin out the malicious traffic. Most of the NIDSes require the network host device to operate on promiscuous mode. This allows the host device to capture each and every packets transferring in the network [37]. Tcpdump (Linux application) and Wireshark (Windows application) are some tools that have ability to capture large traffic flowing through the network. These tools can just monitor and print the network traffic but do possess power to analyze the traffic. Snort is as good example of NIDS. Snort threat signatures are constantly updated and hence, it is considered as an efficient NIDS.

Hybrid Intrusion Detection System

Hybrid Intrusion Detection System comprises both HIDS and NIDS for monitoring and analyzing host event occurring at host computers and network traffic being transmitted in a network respectively. Hybrid Intrusion Detection System is deployed to minimize the compromise in the security level.

2.7 Adaptive Intrusion Detection and Prevention System (AIDPS)

A number of tools exist to control and prevent known malicious actions or attacks in the wireless network. But, what about unknown or newly found attacks? Large numbers of cases are occurring frequently about hacking despite the presence of intrusion detection and prevention tools. This is because, these tools still lack to coin out the unknown malicious actions. An adaptive intrusion detection and prevention tool is supposed to filter out every probable attacks though they are not defined in their database of malicious actions. In fact, these types of tools must be equipped with ability to analyze the network traffic so broadly and at core level that it can assure the network is not compromised at all.

The development of efficient intrusion detection method is under continuous progressive path. Yet, due to ever growing novel attacks and hacks in wireless network, no fully efficient adaptive model has been coined out. Various learning methods are being deployed for the development of such fully adaptive efficient detection tools. Artificial intelligence, machine learning and data mining techniques are being embedded with intrusion detection system with motive of automating adaptive detection method efficiently [33, 38, 39]. Wireless networks are application-driven network where specific protocols exist for specific tasks. This requires intrusion detection system be application specific [33]. However, the models developed have limited scope as they are modeled for certain data sets and for particular problems. In addition, while filtering out the traffic as anomalous traffic, the adaptive intrusion detection tools often mark the valid traffics as malicious traffics, and malicious traffics as general traffics. Such unwanted behaviors are termed as false positive and false negative respectively [35]. An adaptive intrusion detection and prevention system should be able to keep both the false positive and false negative low. However, keeping them low has been headache for the security professionals. Generally, infrequent traffic, though valid, are filtered as malicious traffic, boosting the false positive [35]. Thus, adaptive intrusion detection tools should be trained to build up efficiency in avoiding filtering out valid infrequent traffic as malicious traffic and invalid as valid.

Though a number of techniques are being deployed while building up adaptive intrusion detection and prevention tools, none of the tools are fully reliable. As the tools are developed focusing on specific types of malicious behavior in network, they often fail to mark other types of such harmful traffics during the data transmission.

2.7.1 AIDPS Background-Model Issues

Since, WLAN technology consists of random and unpredictable data traffic, the task of building efficient model has been troublesome to security designers. Reduction in cost and false positives are found considered by most the researchers of adaptive intrusion detection system. The study of different articles [33, 38, 35, 39, 40, 41, 42, 43] on adaptive intrusion detection

system shows the following design issues:

- Difficulty in choosing machine learning algorithm: Different learning algorithms exist to facilitate the IDS to learn self. Markov Chain algorithm, Data Mining technique, Statistic Method and Genetic (Immunity-Based) algorithm are the commonly used machine learning techniques. Cost and effectiveness of learning has been provided central place. Each algorithm has been shown effective for the implementation criteria they are considered for. Mostly, the learning models are targeted towards specific types of intrusion detection. For example, the learning models are either designed for detecting intrusions in system calls or in network traffic. But, genetic learning model has been proved most cost effective as it avoids the need for expensive data sets for training the detection model. Ironically, such algorithm increases the false positives [33, 38, 39].

- Choice of Data Set for Training the Detection Model: For training the detection module to filter out the intrusions in the network system, requires data sets. Mostly the data sets are taken from DARPA [33, 38, 35, 39, 40, 41, 42, 43]. But, these data sets are expensive. Security professionals have thus focused on online learning that is learning from the network traffic automatically. However, the problem of fast convergence needs to be considered. Some data mining techniques focus on building their own database of network traffic or other computer system related data. This database in turn; is deployed for providing the data set for training the detection module. Again the choice of data set depends also upon implementation area of the detection model. That is for what type of intrusions the model has been designed for.

- Assumptions while Designing the Detection Model: The presence of randomness in the network data system seems obstructing the ideal model for adaptive intrusion detection system. Which model has been considered as machine learning algorithm, still most of the security professionals are bound to make some sorts of assumptions. Sometimes, assumptions are made that there exists only certain types of attacks in the network system. Thus, such models are generally overlooking the other types of attacks. Often it is assumed that data sets are provided in time for the detection module to be trained for the new attacks before it gets late. Likewise, assumptions are also made that data are labeled. This significantly increases the costs. On the other hand, detection models require sophisticated training for the unlabeled data.

2.8 Intrusion Detection and Prevention System Tools

It has been more than few decades that the intrusion detection and prevention tools have been brought into existence. However, with

introduction of novel threats day by day, these tools are left obsolete. A revolution is most in the field of intrusion detection and prevention system. The traditional IDPS tools are no more efficient in fulfilling the ever growing security requirements. Currently, concentration has been paid on adaptive intrusion detection and prevention system tools. These tools are supposed to learn about the novel threats that may not exist to the date. At the same time, these tools are expected to reliable exhibiting absolute control over false positive and false negative efficiently. Unfortunately, it is hard to find till today. Only a handful of tools exist that claim themselves to be fully adaptive. Most of them are commercial products. Intense researches are going on in designing such security tools. Snort is one of the intrusion detection tools that has been popular among the security professionals. Several other IDS tools are found based on Snort Threat Signature. Likewise, Cisco Adaptive Intrusion Detection and Prevention Tool is one of the most popular commercial security tools in this field. The following subsections discuss about some of the IDS, IPS and AIDPS.

2.8.1 Snort

Snort is one of the most of popular open source network intrusion detection and prevention system. The tool can perform real-time analysis and logging of network traffic [3, 44]. Snort was built up by Martin Roesch in 1998 and brought among the people by Sourcefire [3]. In general, the tool can detect the attacks like buffer overflows, stealth port scans, SMB probes, OS fingerprinting and CGI attacks. The threats are detected via protocol analysis, content searching and content matching [44].

Snort is designed to operate in three modes, such as [45]:

- **Sniffer Mode:** This mode is selected if the motive is just to read the flowing network traffic in the screen.
- **Packet Logger Mode:** This mode provides the flexibility of saving the network traffic for future analysis.
- **Intrusion Detection System Mode:** This mode is the real implementation of Snort which analyses the network traffic, compares with defined threat signatures and takes action as directed.

Figure 2.12 shows the different components of the snort with quick display of working steps [3]. The components are further discussed below individually.

- **Packet Capture Library:** This is a software module that gathers network traffic flowing through network adapter. For UNIX and Linux Libcap Library is used while for Windows, Wincap is implemented.
- **Packet Decoder:** This part collects the layer-2 frame. Then, it analyses the packet header for anomaly detection. Finally, the packet are decoded for further investigation.

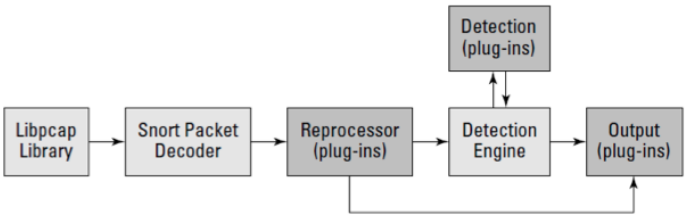


Figure 2.12: *Components of Snort depicting working procedure [3]*

- **Pre-processors:** Pre-processors do the task of arranging and modifying the data before handing over to Detection Engine. In addition, they can detect certain basic of anomalies. Snort has different types of pre-processors. Some of them are discussed below:

  a. **Frag 3 Pre-processor:** It deals with overlapping fragmented packets that might avoid detection or prevention system.

  b. **Stream 5 Pre-processor:** This Pre-processor facilitates snort with state and session awareness. Thus, snort can detect even out-of-state packets resulted from Nmap tool.

  c. **HttpInspect Pre-processor:** It processes the Universal Resource Identifier (URI) through extracting and decoding the hexadecimal or other expressions present in the URI.

- **Detection Engine:** This is the core part among the Snort components. It operates in transport and network layer where it analyzes the packets contents based on defined signature attacks.

- **Output Plug-ins:** This component controls the presentation of output produced after alerting and logging. As it's function, it may produce log reports by logging alert reports or logging in the database or sending message to Syslog Server.

Snort was initially developed for wired network but due to growing concern on wireless security, developers of snort have enhanced the tool in a way that it can operate under WLAN wireless standard 802.11 [46].

2.8.2 Suricata

Suricata is an efficient Network IDS, IPS and Network Security Monitoring engine. The tool was developed by Open Information Security Foundation (OISF) [47]. The developer of the Suricata claims that the tool is as efficient as Snort [3].

Features

The official site of the Suricata recommends to try it for the following three features [47]:

a. **Highly Scalable:** The tool is multi threaded. As such, Suricata balances the load across the sensor nodes on which the tool is configured to be deployed. This provides high speed performance in the network.

b. **Protocol Identification:** Suricata has ability to recognize the most common protocols. This makes possible for the rule writers to create rule based on protocols avoiding the need to have information about ports. The Protocol Identification feature depicts Suricata uniquely as a Malware Command and Control Channel hunter. Further, with dedicated keywords, one can compare protocol fields; ranging from http URI to SSL certificate identifier [47].

c. **File Identification, MD5 (Message Digestion 5) Checksums, and File Extraction:** Suricata is built with ability to identify thousands of file types. In addition, the tool can extract the file flowing in the network in local disk, for later analysis or inspection. Also, Suricata has flexibility of calculating the MD5 checksum that the users in network either can to maintain or discard from the network.

Besides, the tool has a number of additional features and can operate in multiple platforms like Windows, Linux, Mac, FreeBSD etc [3, 47].

2.8.3 OSSEC

OSSEC is a host-based intrusion detection system that is provided for free. The tool provides anomaly detection system through log analysis, file integrity checking, and rootkit detection. In addition, OSSEC monitors policy, does real-time alerting and provides active response. The tool is compatible with most of the operating systems [48].

Originally, OSSEC was brought into existence by Danial B. Cid [48]in order to overcome the scalability problem of Tripwire. These days, it is supported by a company named Trend Micro. OSSEC performs profile and signature based analysis to detecting intrusions [48, 49].

Features

OSSEC is accumulates most of the aspects of HIDS, log monitoring and SIM/SIEM in a simple way but as powerful tool. The following are the key features of the OSSEC tool [48]:

a. **File Integrity Checking:** Through File Integrity Checking (often termed as File Integrity Monitoring (FIM)), OSSEC checks for any changes in file, directory or even registry. If any such instances do exist, then, OSSEC generates alerts. Such changes can either be attacks or simply misuses.

b. **Log Monitoring:** OSSEC can read and analyze the log files created by the operating system. Any suspicious actions suggested by these log files are alerted by the tool. These log files may record information about application installations, changes in the firewall rules etc.

c. **Rootkit Detection:** Hackers or anomalies always intend to hide their malicious actions, but through Rootkit Detection, OSSEC can reveal such malicious actions that might hamper the computer system.

d. **Active Response:** OSSEC is built with feature of Active Response. This makes possible to take actions immediately whenever threats are suspected in the network. Thus, one time configuration is enough to take real time action in the process of combating the anomalous activities.

2.8.4 Bro

Bro is a network-based open source intrusion detection system. Thus, the primarily focus of Bro is on network security monitoring. However, the tool puts some weight on analysis of general network traffic too. Bro was developed by Vern Paxson [3] 15 years ago. Currently it is backed by Paxson with his team at International Computer Science Institute, Berkeley, CA and the National Center for Supercomputing Applications, Urbana-Champagain, IL [50]. Bro's policy scripts are created by it's own Bro Scripting Language. Bro has a tool named BroControl which assists in managing multiple Bro nodes in parallel. Bro is also a single threaded tool [3, 51].

Features

Bro comes with the following features some of which differentiate it from the rest of the intrusion detection system [50]:

a. **Adaptable:** Bro provides the site-specific monitoring policies through domain-specific scripting language.

b. **Efficient:** Bro concentrates on high-performance and wide deployment platform.

c. **Flexible:** Bro is far from traditional threat signature definitions and is not based on any single detection methods.

d. **Forensics:** Bro logs the network traffic that is under monitoring and provides higher level of presentation.

e. **In-depth Analysis:** Bro can analyze many protocols and can perform semantic analysis at application layer at efficiently.

f. **Highly Stateful:** Bro keeps track of application layer state while monitoring the traffic.

2.8.5 Tripwire

Tripwire is a host based intrusion detection system that checks for files and directories integrity. The tool checks for alterations in such files and directories with automated cron job. Any misconducts in file integrity are notified through email. Tripwire constantly monitors the system for any

possible changes. In addition, it facilitates with prompt recovery by filtering out only the corrupted files for remaking [52].

Tripwire typically uses the baseline database of the file locations and modification dates for comparing the files directories integrity. This baseline is created by with snapshots of the files and directories while in secure state [52, 53].

2.8.6 Sourcefire Next-Generation Intrusion Prevention System (NGIPS)

With focus on overcoming the shortcomings of first generation IPS, Sourcefire has developed the Next-Generation Intrusion Detection System (NGIPS). The tool is endorsed by Gartner [54]. The NGIPS provides the enhanced capabilities required to secure computer network from emerging threats. The concept behind the tool is contextual awareness about network traffic, systems and applications, users and other network components. This contextual awareness provides quick recognition of threats and takes appropriate actions. NGIPS is also claimed to be cost effective [54]. Unlike, other tools discussed above, Sourcefire NGIPS is a commercial product.

Features

In addition to conventional features present in the first generation IPS, Sourcefire NGIPS has the following features [54]:

a. **Inline Bump-in-the-Wire Configuration:** Sourcefire NGIPS does not disrupt the network traffic even the tools encounters hardware or software failure. The tool has option of operating as "fail-open" which ensures network traffic flow though any detection may not occur.

b. **Application Awareness and Full-Stack Visibility:** Sourcefire claim "Sourcefire NGIPS is the first and only IPS provider to offer passive, real-time network intelligence gathering" [54]. The tool can perform the task of limiting the use of operating system and related applications in the network. Thus, it shrinks the area of possible attack in the network, thereby, reducing the volume of risk.

c. **Contextual Awareness:** Sourcefire NGIPS can prioritize threats detection and take action accordingly or even may not take action if not needed. The tool can gather information about existing and network devices added in the network, can keep track of various network applications like operating systems, VoIP systems, printers etc., and identify the users of the network. The tool can then create scenario proactively before any such network components may create intrusions. Thus, can take action prior to threat encounters.

   In addition, Sourcefire NGIPS is featured with efficient automated IPS tuning as the tool keeps track information of every network elements. The tool is also embedded with features to get integrated with other network components.

d. **Content Awareness:** In addition to the ability of filtering out the traditional threats like worms, trojans, buffer overflows and DoS attacks, Sourcefire NGIPS is capable of detecting threats that might emerge from the content of the files like PDFs and Microsoft Office files.

2.8.7 Cisco Adaptive Wireless Intrusion Prevention System

Cisco Adaptive Wireless Intrusion Prevention System is an advanced security software for combating wireless threats like network anomalies, unauthorized accesses and RF attacks [55]. The Cisco Wireless IPS is one of the constituents of the Cisco 3300 Series Mobility Services Engine platform with location-aware technology. The tool is provided with proactive threat detection capability [55].

Features

Cisco is one of the advanced tools in the field of adaptive wireless intrusion detection and prevention system. It comes with the following features [55]:

a. The tool provides the complete wireless anomaly detection and preventive actions in the wireless network infrastructure.

b. The tool provides cost-effective security solutions in the wireless network.

c. The tool ensures the wireless security through rogue access point monitoring, detecting ad-hoc connection and detecting wireless hacking. Additionally, it does the task of self optimization, security management and reporting.

2.8.8 Kismet

Kismet is a WLAN security tool which can sniff and check for intrusions in the wireless network. Kismet also provides security breach check in other than 802.11 wireless standard. Particularly, it serves for 802.11b, 802.11a, 802.11g and 802.11n network traffics. The only requirement for Kismet to get deployed is that wireless network card should support monitoring mode [56].

Kismet passively detects and collects the network traffic. It checks for the hidden networks and non-beaconing networks through such collected data packages [56].

Features

Kismet is one of the few open source wireless intrusion detection tools. It has the following features while serving as wireless intrusion detection system [56]:

a. It functions as both stateless and stateful intrusion detection system and can detect threats like fingerprints (single packet attack) and trends like unexpected probes, disassociation flood, etc.

b. Kismet can easily be integrated with other tools like Snort. Such tools can process the Kismet captured data traffic for further analysis.

c. Kismet can operate in mobile or channel hopping installations, but; accuracy may be compromised.

2.8.9 RFProtect Wireless Intrusion Protection

RFProtect Wireless Intrusion Protection is developed by Aruba Networks. The tool detects the wireless threats in the form of either wireless attack, impersonations or intrusions. Any mismatches with defined signatures are filtered out as threats in the wireless network. Unlike many other commercial products, the RFProtect is integrated in the wireless network system, thereby, avoiding the need for dedicated wireless sensors [57]. Hence, this product is comparatively cost effective [57].

Features

The features mentioned for RFProtect are not new in the field of intrusion detection system. But, still they worth much when it comes to wireless security. The following features are enlisted by Aruba Networks for RFProtect [57]:

a. **Integrated Wireless Intrusion Detection and Prevention:** RFProtect is directly integrated within the wireless network device, thus it obviates the need for separate wireless overlay IDS and sensors.

b. **Automatic Threat Mitigation:** RFProtect keeps track of unauthorized clients and ad-hoc networking through forensic data evaluation. The tools blocks such clients from being connected to the network.

c. **Customizable Security Polices:** This feature adds flexibility of defining the security policies as per deployment needs. The criteria can be based on location, device or configuration.

d. **Automated Compliance Reporting:** RFProtect does the task of reporting about the actions performed automatically. Thus, it saves time and reduces complexity avoiding user intervention.

Figure 2.13 provides the brief overview of all the tools discussed above.

Tool	Platform	Type	N/W	Threat	Source	Detection
Snort	Almost all	NIDS	Wired/ wireless	Buffer overflow, stealth port scan, SMB probes, OS fingerprinting, CGI attacks	Open source	Rule based, anomaly based
Suricata	Most	NIDS	Wired	Known threats	Open source	Rule based, anomaly based
Ossec	Most	HIDS	Wired/ wireless	File integrity breach, rootkit detection	Open Source	Rule based
Bro	Unix	NIDS	Wired	N/A	Open source	Pattern based
Tripwire	Most	HIDS	Wired	File and directory integrity breach	Open source	Audit assessment
Kismet	Almost all	IDS	Wireless	Fingerprints, unexpected probes, dissociation flood	Open source	Packet sniffing
RFProtector	N/A	IDS/ IPS	Wireless	DoS Attack, Man-in-the –middle attack, unauthorized access, rogue AP	Commercial	Rule based
Cisco Adaptive IPS	N/A	NIDS	Wireless	Rogue Aps, DoS attack, authentication, man-in-the-middle attack	Commercial	Rule based, anomaly based
Source-fire NGIPS	N/A	IDS	Wired/ Wireless	Known, adaptive	Commercial	Contextual awareness based anomaly

Figure 2.13: *Table briefing the IDS/IPS discussed above*

2.9 Network Simulators

Simulators are the tools that provide the figurative and functional representation of a system. The simulator even demonstrates the internal working procedure of the system components which in reality are hidden by the real devices. Simulators enlighten the hidden working principles that are generally known to just experts of the related systems. More importantly, simulators provide the platform for testing applicability and reliability new systems before they are deployed in the real environment. Thus, simulator prevents from the real risk of failure. In addition, it saves the cost of testing new systems obviating the need for buying infrastructures before hand.

Generally, simulators are implemented for simulating the applicability of new systems and sophisticated systems. Computer network is one of such sophisticated systems where simulators are highly deployed. These network simulators have made it possible to check for the implementational feasibility of different computer networks ranging from pervasive sensor networks to satellite networks. Different network simulators are also deployed to simulate various wireless sensor networks. WSN (Wireless Sensor Network) simulators are mainly used to confirm the applicability of new protocols in the wireless sensors network [58]. However, these simulators are still not completely built up to simulate the sensor networks fully, specially, not for 802.15.4 networks. The following discussion provides the overview of different network simulators that can be deployed for simulating wireless sensor network.

2.9.1 Network Simulator -2 (NS-2)

Network Simulator version 2 or NS-2 is one of the oldest network simulator. This is an open source tool and initially developed for simulating NS-2. Defense Advanced Research Projects Agency and National Science Foundation are behind NS-2 improvement. The tool is based on object oriented programming language, typically C++ and built primarily for Linux environment [59, 58]. NS-2 tool provides well defined online documentation.

NS-2 is not facilitated with graphical interface, thus, users need to have sound coding or scripting skills. Since, NS-2 is originally developed for IP network, it also lacks the proper functionality for wireless sensor network [58]. The tool falls short of consistency and accuracy. In addition, the tool cannot accommodate more than 100 sensor nodes, thus bears scability problem too. However, NS-2 can be used to simulate simple wireless sensor network.

2.9.2 Avrora

Avrora is a Java based open source simulation tool developed by University of California, LA Compilers group [60]. The tool can efficiently simulate wireless sensor network but misses graphical interface. Avrora does not provide support for network management as it does not hold network

communication tool [58]. Avrora is faster and scalable simulation tool. The tool can simulate more than 1000 nodes at once. As the tool is developed with Java, it provides flexibility too.

2.9.3 OMNeT++

OMNeT++ is a network simulator built in C++. It can be found in both free licensed version for academic and non-profit research purpose and commercial for others. However, it provides broad open source framework and mode. The tool can operate on Linux, Windows and Unix [61]. The tool is highly advanced and sophisticated.

The OMNeT++ is efficient for simulation both wired and wireless network. It supports wireless sensor network and provides free model named MiXin for particularly simulating ZigBee network. The OMNeT++ provides graphical interface. One can easily simulate even power consumption in wireless sensor network. However, as large team is behind development of the tool, often the compatibility problem arises while simulating with different models [58]. The graphical interface provides efficient platform for debugging the simulation but still the OMNeT++ requires sound knowledge of programming (C++) while simulating the advance computer network.

2.9.4 Opnet Modeler

Opnet Modeler Wireless Suite is an efficient simulator for wireless network. The model can be implemented for simulating a wide variety of wireless networks [30]. One of the most promising feature of the OPNET Modeler is it's graphical interface which provides users with easy implementation, eliminating the burden of working with background coding. This feature has helped it surmount other network simulators. The OPNET Modeler is basically a commercial product. However, for the non-profitable research and for the academic use, the OPNET provides free six-month license [30].

The OPNET supports even personal area networks like Bluetooth, ZigBee etc. It also supports Satellite simulation. The model can be deployed for analyzing the end-to-end functionality and examine network performance from small wireless network like Bluetooth network to Satellite network [30]. The official website for the OPNET [30] writes that the simulator has the following features:

- It is the fastest simulator
- It has a complete library of hundreds of network protocols and vendor device models.
- It is a scalable and customizable wireless modeler.
- IT provides integrated, GUI-based debugging and analysis.
- It provides open interface providing path for integrating external models, libraries and even simulators.
- It even facilitates the realistic application modeling and analysis.

Chapter 3

Approach

This chapter provides the overview on what experiments will be carried out and how they will be carried out to address the objective of this research. Details on these are mentioned below.

3.1 Methodology

To resolve the issues mentioned in the problem statements above, the overall task will be divided into three sections. In the first section, attacks of concern will be generated, the second section will analyze the attack and the third section will make attempts to detect and prevent the attack. To accomplish these tasks, two lab set-ups will be made in two environment.

As the WBAN technology is still under research, no concrete procedures are available to carry on the tests. Considering the complexities, that may arise due to unavailability of hardware and firmwares, device-specific tests other than the available devices in the ASSET lab, will be carried on a wireless network simulator. For example, DoS attacks can be accomplished through different techniques. Often attackers deploy special wireless signal jamming device which are easily available in market. In addition, devices with specifications, similar to the devices used in the network might be deployed to create DoS attacks. In order to tests all these possible attacks, simulation work will be carried out as it avoids the need of acquiring real devices for experimenting.

Every planned tasks cannot be accomplished through simulator alone. All other feasible tests will be carried on the ASSET laboratory environment. Thus, simulator and physical lab will be two platforms to accomplish the desired tests. The most threatening attacks in the WBAN, that is DoS attacks, will be carried through wireless network simulator named the OPNET Wireless Modeler Suite. Eavesdropping, Integrity and Replay Attack will be tested in the physical lab.

The following section discusses on different hardware and software tools considered for the thesis work and plan for the executing the task. The reason behind selection of hardware and software, and procedures are also be mentioned.

3.1.1 Hardware and Software Tools

As this thesis work is based on 802.15.4 network, different hardware other than commonly used devices like computers, routers and switches; are also needed. The ASSET lab-set-up contains the following hardware devices as mentioned in Table 3.1 [62]. Among them Telosb Tmote Sky and Atmel AVR Raven ATAVRRZUSBSTICK are added for to facilitate security analysis work. Specifications are adopted from [63, 64, 65].

Table 3.1: *Hardware Specifications*

Hardware	**Specification**
Laptop	
	Memory: 4 GB Processor : Intel Core 2 Due OS : Ubuntu 12.04 32-bit
Shimmer Sensor	
	I/O : 3 colored led indicators RAM : 10 KB Flash : 48 KB Frequency : 8 MHz
Shimmer Span	
	I/O :3 colored led indicators Processing : MSP430F1611 CPU Communication : TIC2420 802.15.4 radio transceiver Form Factor : USB flashdrive
Telosb Tmote Sky	
	I/O : 16-pin expansion support and optional SMA antenna connector Radios : 802.15.4 Radio CPU : MSP430F1611 CPU Datasheet/Users Guide Storage : Uses the ST M25P80 40MHz serial code flash for external data and code
ATAVRRZUSBSTICK	
	Frequency : 2.4 GHz Interface Type: USB Category : ZigBee/802.15.4 Development Tools

Figure 3.1 and Figure 3.2 show the pictures of sensor devices that have been deployed.

Figure 3.1: *A Shimmer Span and A Shimmer End Device*

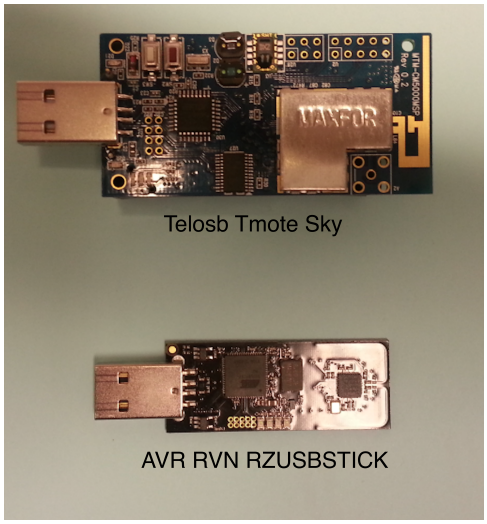


Figure 3.2: *A Telosb Tmote Sky and A Atmel AVR RAVEN RZUSBSTICK sensors*

Table 3.2 provides an overview of the hardware and their purposes.

In order to make devices mentioned above work, different types of firmwares are needed. Since experiments will be conducted in simulator, a simulation software will be used in addition. Table 3.3 provides the quick vision of different types of software and firmwares that will be used with their purposes.

Table 3.2: *Hardware that are planned to be used in experiments*

Hardware	Quantity	Purpose
Laptop	1	Collecting data, monitoring and analyzing the results of the experiment
Shimmer Span	1	Collecting data from Shimmer nodes
Shimmer node	5	Sensing and preparing data for Shimmer node
Telosb	1	Emulating the 802.15.4 network data for Wireshark
AVR Raven	1	Generating attacks in the 802.15.4 network

Table 3.3: *Software and firmwares that are planned to be deployed in experiments*

Software/firmware	Device Associated	Purpose
OPNET Modeler	Laptop	Carry on simulation work
Tiny OS	Laptop	Provide communicating platform for sensor devices
Wireshark	Laptop	Analyze 802.15.4 traffic
PPPSniffer	Telosb	Feed 802.15.4 data to Wireshark
KillerBee	AVR RAVEN	Create attack on 802.15.4 network
Goodfet	Telosb	Sniff and analyze 802.15.4 traffic
Scapy	Telosb	Decode and dissect 802.15.4 traffic

3.1.2 Plan and Procedure

1. **Generation of Attack:** Different types of attacks will be implemented as mentioned earlier in two parts as simulation work and physical lab work.

    i. **Simulation Work:**

    As a simulation work, the simulation of DoS attack will be performed in two scenarios. An alternative approach to conduct simulation work is also mentioned below:

    a. **Scenario 1:** The first scenario will conduct experiments on DoS attack that may arise due to malicious devices or misbehaving devices within the network. The malicious node will generate large volume of traffic, targeted to the base station. This scenario represents the environment for

both intentional or unintentional resource consuming malicious tasks, resulted from within the network. One of the devices, will be misconfigured to consume more network resources.

b. **Scenario 2:** Here, jammer nodes, which create specific interference in the wireless network, will be deployed. These jammer nodes may also result in congestion in the network, resulting loss of packets. Jammer nodes will be created via simulator. This scenario will represent the intentional DoS attack that might be encountered through different easily available wireless signal jamming devices.

ii. **Physical Laboratory Work:** The lab set-up will include a network of five Shimmer Nodes, a Shimmer Span Module and a laptop as analyzer. The nodes will be configured with star topology. As mentioned earlier, eavesdropping, integrity and replay attack will be tested on physical laboratory. All the mentioned malicious tasks will be tried to accomplish through the modification on the firmware configured in the Shimmer Modules and make it operate as malicious node. The scenario will represent a case where hackers and attackers introduce their misbehaving devices in the network and try to sniff, modify or regenerate the traffic.

2. **Analysis of Attack**

   Wireshark is the one of the commonly used packet analyzer. This tool will be used to analyze the traffic generated by both the simulator and the physical lab. Typically, Wireshark is developed for IP packet analysis. Thus, it is not able to analyze the packet generated by 802.15.4 network directly. The packet generated by the ZigBee network (802.15.4 standard) is different from IP network traffic. So, the PPPSniffer will be installed in one of the Shimmer node to function it as bridge to emulate the 802.15.4 traffic to pcap traffic that Wireshark understands.

3. **Detection of Attack:** Snort and Kismet are the intrusion detection tools that will be implemented as intrusion detection systems. Snort is typically developed as network intrusion detection system for the wired network. Thus, an attempt will be made to find out if the Snort functions in the traffic converted by the PPPSniffer. Else, as an alternative attempt, traffic analyzed by the Wireshark or other packet analyzer will be fed to snort for offline reading. Kismet is developed for 802.11 based wireless network. Thus, similar attempt will be made to figure out if the Kismet can recognize the traffic emulated by the PPPSniffer. If the tools are able to detect intrusions, comparison of their performance will be made based on their ability to detect the attacks of interest or else reasons behind their inabilities will be discussed.

3.1.3 Alternative Approaches

Since, the hardware and software that are going to be implemented are unusual, the proposed plan may not produce the desired output. Possibilities do exist that these hardware and software may not be compatible with each other or not feasible in the platform under consideration. The following alternatives are provided for both hardware and software:

- **Alternative Simulator:** Network Simulator OPNET Modeler Wireless Suite, considered for the simulation work, is sophisticated though it provides graphical interface. As ZigBee network is still in nascent stage, the considered the OPNET Modeler has ZigBee implementation but not fully functional as expected. In case; this simulator creates complications, the OMNeT++ will be considered as alternative for simulation work. The OMNeT++ also supports 802.15.4 network with graphical interface.

- **Alternative Devices:** The proposed plan may not produce the desired output as possibilities exist that these hardware and software may not be compatible with each other or not feasible in the platform under consideration. Telosb Tmote Sky will be an alternative hardware. This TelosB Tmote Sky will be configured with the Goodfet firmware and KillerBee firmware. As a result, this device may assist in sniffing the network traffic and also making replay attack and injection attack.

- **Alternative Package Analyzer:** In case, Wireshark is not able to analyze the traffic generated by ZigBee network, TCPdump will be considered as an alternative. Since, TCPdump is originally developed for Linux environment, it functions as package analyzer after necessary modification is made on the ZigBee traffic.

- **Alternative Approach in Intrusion Detection:** As the proposed IDS are not meant to work on ZigBee network, they may face compatibility issues. In order to emulate the traffic into IP packet format, WSBridge will be considered as an alternative. This firmware will be configured with Telosb Tmote Sky to make it operate as 802.15.4 traffic to IP packet emulator.

  In case, these intrusion detection tools do not found feasible at all, theoretical approach will be followed. This theoretical approach will illustrate the need for the intrusion detection system in Wireless Body Area Network. The approach will discuss on the reason behind inability of the IDS tools to function on 802.15.4 network. Finally, the approach will also propose the possible techniques to accomplish the task.

3.1.4 Summary of Proposed Methodology

In short, the following task will be executed:

a. **Simulation Work**

i. *DoS Attack from Misbehaving Node*

- Create a ZigBee simulation platform similar to ASSET lab
- Create a misbehaving node altering the parameters of one of the sensor node
- Analyze the effect of the misbehaving node through simulator and Wireshark
- Analyze the traffic generated by misbehaving node through Snort and Kismet
- Propose the better tool based on their performance in the attack environment considered

ii. *DoS Attack from Jammer Node*

- Create a ZigBee simulation platform similar to ASSET lab
- Create a jammer using simulator node model and deploy it in the simulation network
- Analyze the effect of the jammer node through simulator and Wireshark
- Analyze the traffic generated by misbehaving node through Snort and Kismet
- Propose the better tool based on their performance in the attack environment considered

b. **Physical Laboratory Work**

- Create a network of Shimmer Nodes, Shimmer Span Module and a laptop using star topology
- Create packet sniffer, packet injector and packet replay attacker using the Shimmer Node and introduce them into the network
- Analyze the possible threats generated by attacker node through a set of PPPSniffer configured device and Wireshark
- Analyze the intrusion generated the attacker node through Snort and Kismet
- Propose the better tool based on their performance in the attack environment considered

Chapter 4

Result and Analysis

This chapter discusses on the experimental setup, both simulation and physical lab setup, implemented for the tests, details on procedure and methodology followed and the results obtained from both experiments. Each section is discussed under their respective topics as mentioned below. Analysis of the result is conducted at the latter part of this chapter.

4.1 Experimental Setup I

The experimental set-up for the task was designed as proposed. The tests were carried on in the simulator - OPNET Modeler Wireless Suite, version 17.5. The figure 4.1 represents the general experimental setup designed in the simulator. A platform of 50m*50m area was created to conduct simulation experiments. The network consists of a ZigBee coordinator, a ZigBee router and 5 ZigBee end devices. The end devices were the sensors that collect data from physical environment based on motion of the body parts. The destination of traffic from these devices was ultimately the *Coordinator*. The default parameters were selected for all the devices except the destination of traffic for each device. All the end devices were set to send the data gathered to the *Coordinator* through router. The *Coordinator* was set with destination as router. Figure 4.2 shows the parameter selection for the *Coordinator* and end devices respectively. The simulation task was accomplished in two scenarios. In both scenarios, focus was made on load experienced by the *Coordinator* and the packets dropped by the *Coordinator* under such loads. Each experiments in the simulation work was simulated for 7 hours to resemble the physical lab experiment-time duration.

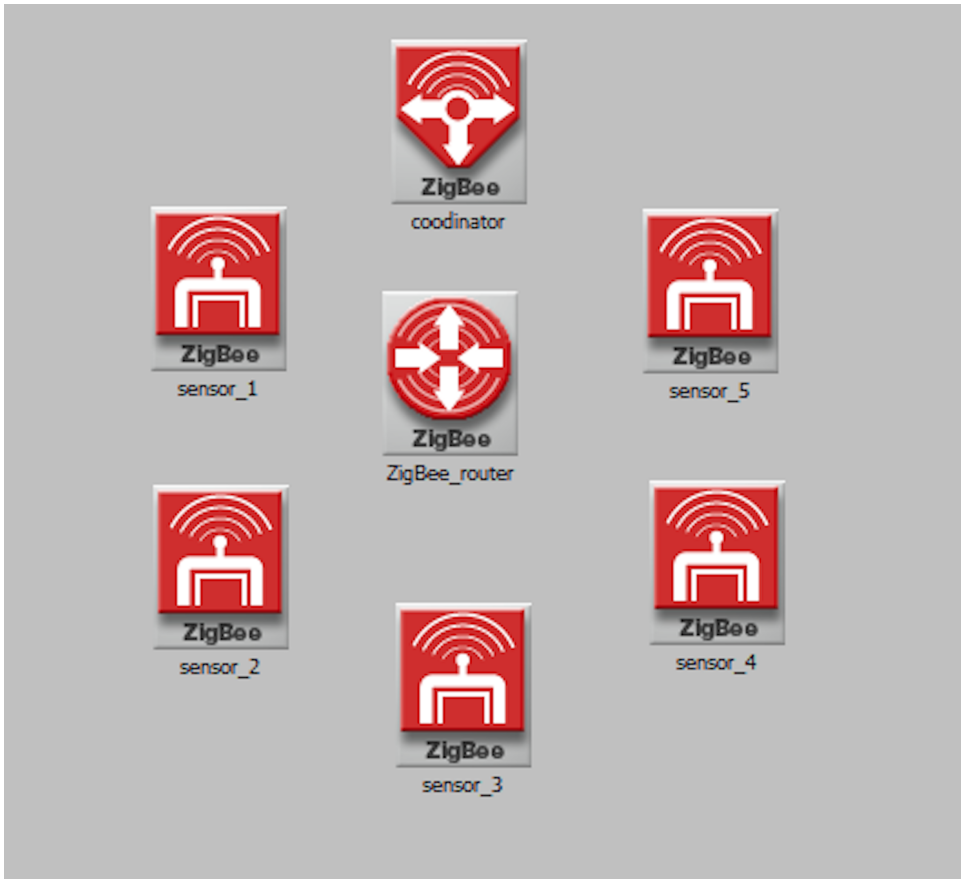
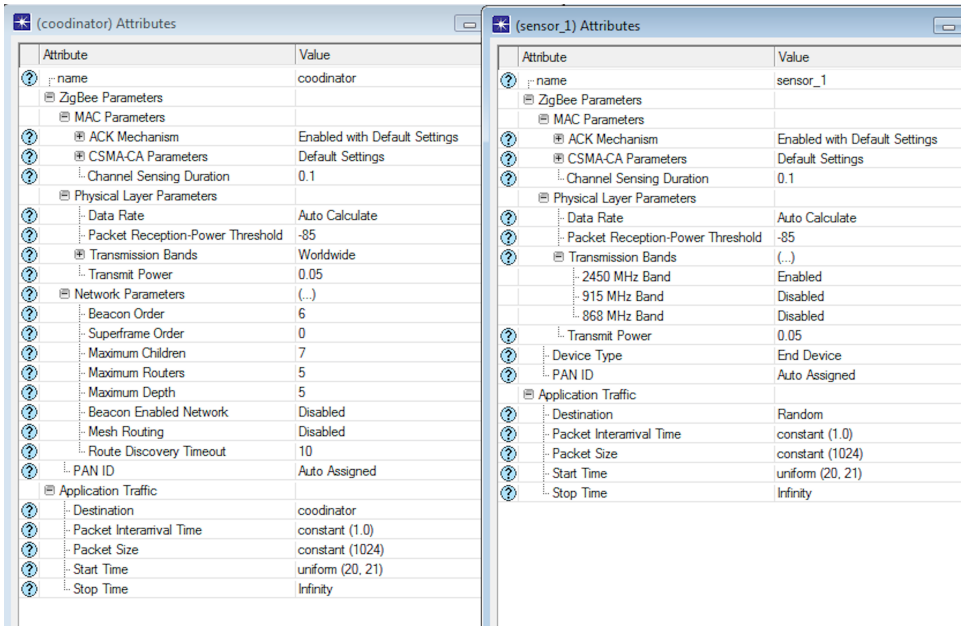


Figure 4.1: *General simulation network setup*



(coodinator) Attributes

Attribute	Value
name	coodinator
ZigBee Parameters	
MAC Parameters	
ACK Mechanism	Enabled with Default Settings
CSMA-CA Parameters	Default Settings
Channel Sensing Duration	0.1
Physical Layer Parameters	
Data Rate	Auto Calculate
Packet Reception-Power Threshold	-85
Transmission Bands	Worldwide
Transmit Power	0.05
Network Parameters	(...)
Beacon Order	6
Superframe Order	0
Maximum Children	7
Maximum Routers	5
Maximum Depth	5
Beacon Enabled Network	Disabled
Mesh Routing	Disabled
Route Discovery Timeout	10
PAN ID	Auto Assigned
Application Traffic	
Destination	coodinator
Packet Interarrival Time	constant (1.0)
Packet Size	constant (1024)
Start Time	uniform (20, 21)
Stop Time	Infinity

(sensor_1) Attributes

Attribute	Value
name	sensor_1
ZigBee Parameters	
MAC Parameters	
ACK Mechanism	Enabled with Default Settings
CSMA-CA Parameters	Default Settings
Channel Sensing Duration	0.1
Physical Layer Parameters	
Data Rate	Auto Calculate
Packet Reception-Power Threshold	-85
Transmission Bands	(...)
2450 MHz Band	Enabled
915 MHz Band	Disabled
868 MHz Band	Disabled
Transmit Power	0.05
Device Type	End Device
PAN ID	Auto Assigned
Application Traffic	
Destination	Random
Packet Interarrival Time	constant (1.0)
Packet Size	constant (1024)
Start Time	uniform (20, 21)
Stop Time	Infinity

Figure 4.2: *Parameters selection for ZigBee coordinator and end device sensors*

4.1.1 Scenario 1:

The experimental setup for the scenario 1 was as shown in Figure 4.3. The experiment was initiated with normal operation where all the end device sensors send normal traffic to the *Coordinator*. Later on, a misbehaving node was created and implemented as attacking node for the *Coordinator*. Initially, all nodes sent constant packets of size 1024 bits. But, the attacking node was made to send larger traffic. In each test, the size of the packet was increased by 1024 bits. The experiment was carried on till the packet size reached 40960 bits. Figure 4.4 exhibits the effect seen on load and packets dropped by the *Coordinator* as a result of the misbehaving node. Likewise, Figure 4.5 shows the load increasing on *Coordinator* with increase in packet size sent from the misbehaving node.

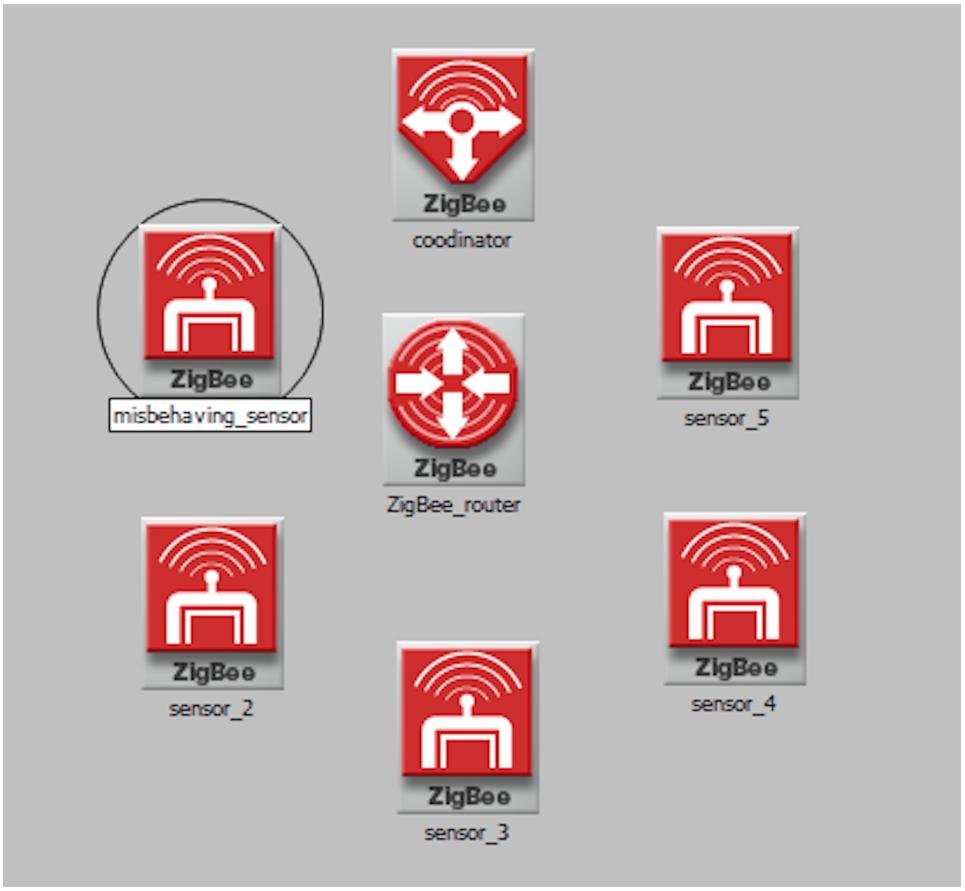


Figure 4.3: *Network setup with misbehaving node*

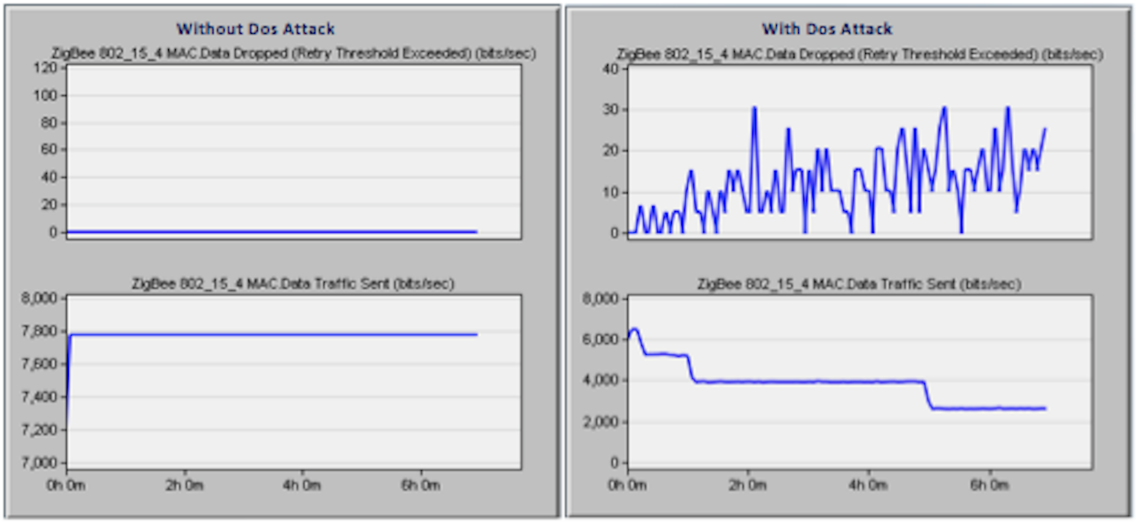


Figure 4.4: *Load on coordinator before and after introduction of misbehaving node*

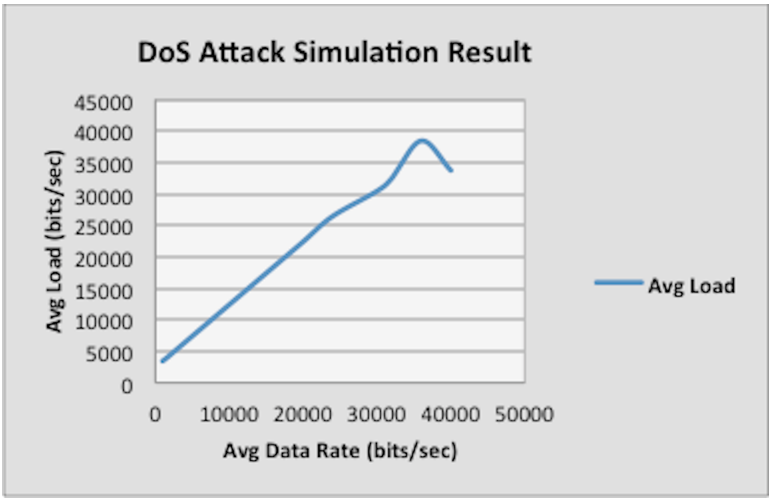


Figure 4.5: *Pattern of load-change on coordinator with increased packet size on misbehaving node*

4.1.2 Scenario 2:

In the second lab setup, a jammer node was introduced instead of misbehaving node. The jammer node was place as shown in Figure 4.6. The jammer node was selected from the standard jammer nodes present in the simulator. Experiments were then carried on to find out the effects on *Coordinator* before and after the introduction of jammer nodes. Figure 4.7 provides overview of packets dropped and load encountered by the *Coordinator* under both conditions.

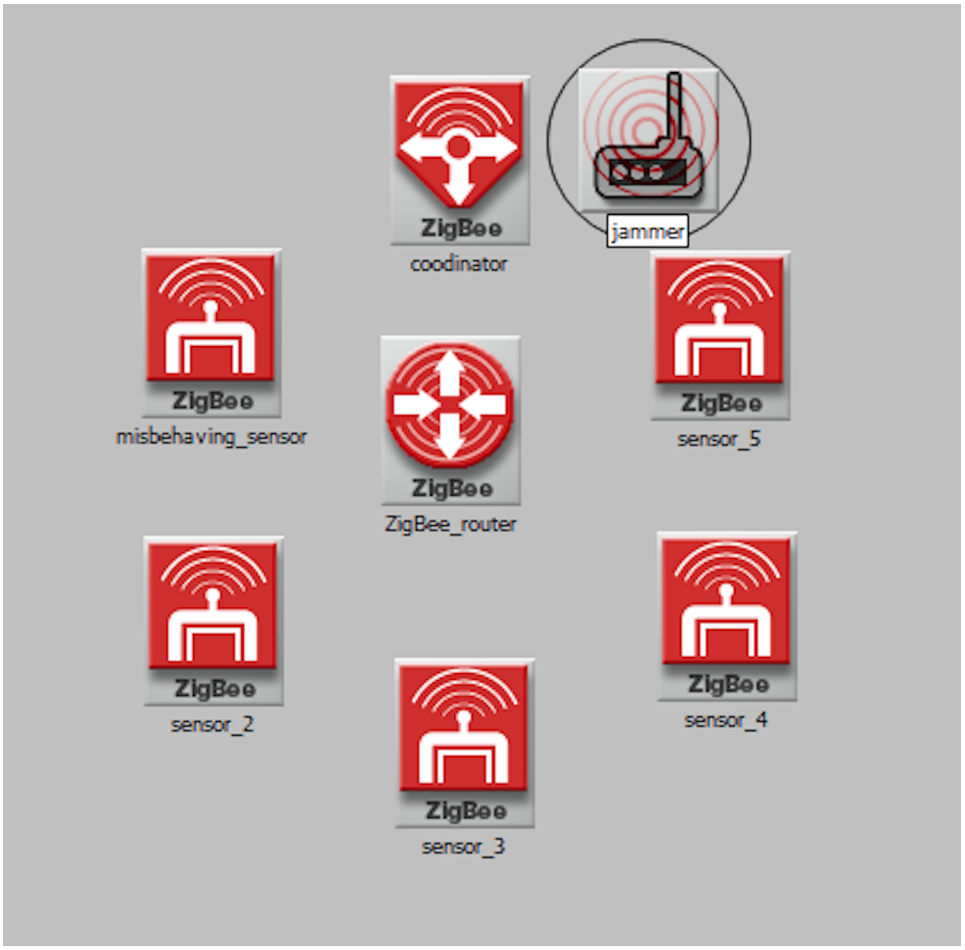


Figure 4.6: *Network setup with one jammer node*

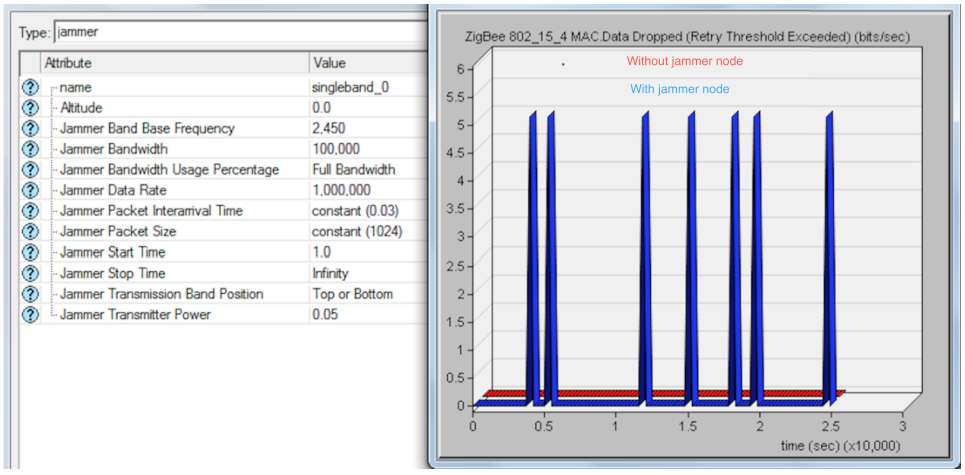


Figure 4.7: *Attributes selected for jammer node and traffic lost by the Coordinator*

4.2 Experimental Setup II

The second lab setup consisted of three computers, one Shimmer Span module as a *Coordinator*, five Shimmer sensors, one Telosb Tmote Sky

transceiver one Atmel AVR Raven transceiver. Shimmer Span module, KillerBee device and the Telosb Goodfet device were configured in three different computers. The sensors and the Span module were organized with star topology. The sensors were put on the body. The sensors used to collect gyroscopic data based on the body movements. Those sensed data were transferred to the Span module and the module would then supplied the data to the computer, it was attached with.

Different tests were conducted with focus on packet network scanning, packet sniffing and packet injection. The Telosb device; configured with the Goodfet firmware was made to sniff the 802.15.4 data flowing in the network. Likewise, Atmel AVR Raven was configured with KillerBee firmware. The device could scan the 802.15.4 network, dump the network traffic and make replay attack. The attacks were accomplished in three scenarios:

4.2.1 Scenario 1:

In the first lab experiment, the KillerBee device was deployed as attacking node and the Telosb Goodfet device was implemented as monitoring node. KillerBee device was deployed to scan the 802.15.4 network. Through *zbstumbler* command, the device generated beacon request broadcasts. Then, the device recorded the PAN-id of the responding devices and the channel number used by them. The beacon requests sent from the KillerBee device was monitored through the Telosb Goodfet device. This Goodfet device was set to sniff the packets flowing in the network in all channels. Figure 4.8 shows an instance of beacon request broadcast sent from the KillerBee device.

```
Scanning channels [11,26].
26:  71 41 88 e2 22 00 00 00 06 00 3f 7f c9 e3 3d 07 8f 04 ae 06 11 08 19 07 1
d 08 ad 09 34 07 a5 04 b0 06 19 08 21 07 1e 08 ac 09 2a 07 99 04 b0 06 11 08 1
a 07 20 08 a9 09 35 07 a3 04 b1 06 13 08 18 07 1a 08 a9 09 2c 07 a5 04 ad 06 0
c 08 0b 07 20 08 a9 09 2d 07 95 04 ae 06 17 08 17 07 1d 08 ad 09 2d 07 9f 04 a
f 06 12 08 17 07 24 08 ab 09 4e 39
14:  0a 03 08 03 ff ff ff ff 07 45 25
18:  0a 03 08 17 ff ff ff ff 07 59 77
26:  71 41 88 27 22 00 00 00 06 00 3f 7f ca 28 30 07 9c 04 bb 06 12 08 19 07 1
c 08 aa 09 27 07 95 04 b1 06 18 08 1b 07 19 08 a9 09 2f 07 9b 04 b1 06 10 08 1
2 07 16 08 a7 09 2b 07 a2 04 cd 06 1a 08 1e 07 1d 08 ad 09 38 07 9d 04 b2 06 1
5 08 1f 07 1b 08 aa 09 28 07 a6 04 b6 06 19 08 23 07 22 08 ad 09 25 07 9f 04 b
8 06 12 08 1e 07 1d 08 ac 09 8a e7
26:  71 41 88 35 22 00 00 00 06 00 3f 7f ca 36 30 07 a2 04 9c 06 14 08 16 07 1
f 08 ae 09 30 07 99 04 bb 06 15 08 1b 07 1c 08 aa 09 35 07 89 04 ba 06 19 08 2
1 07 1d 08 ac 09 25 07 99 04 ab 06 11 08 1a 07 1d 08 ac 09 2e 07 a6 04 bb 06 1
1 08 17 07 1d 08 ac 09 3f 07 96 04 b1 06 19 08 20 07 22 08 ad 09 44 07 9a 04 b
3 06 13 08 1e 07 1e 08 ac 09 57 f9
26:  71 41 88 43 22 00 00 00 06 00 3f 7f ca 44 3b 07 90 04 b2 06 17 08 11 07 1
```

Figure 4.8: *Beacon request sent from the KillerBee device for scanning the network*

The embedded code for the sniffing command (goodfet.ccspi) was modified so that it could decode and dissect the 802.15.4 hex traffics to understandable format. Figure 4.9 depicts the dissected beacon request that is highlighted in Figure 4.8. Data in the blue box represents the beacon request and that in the orange box represents the channel number that the beacon request is generated at.

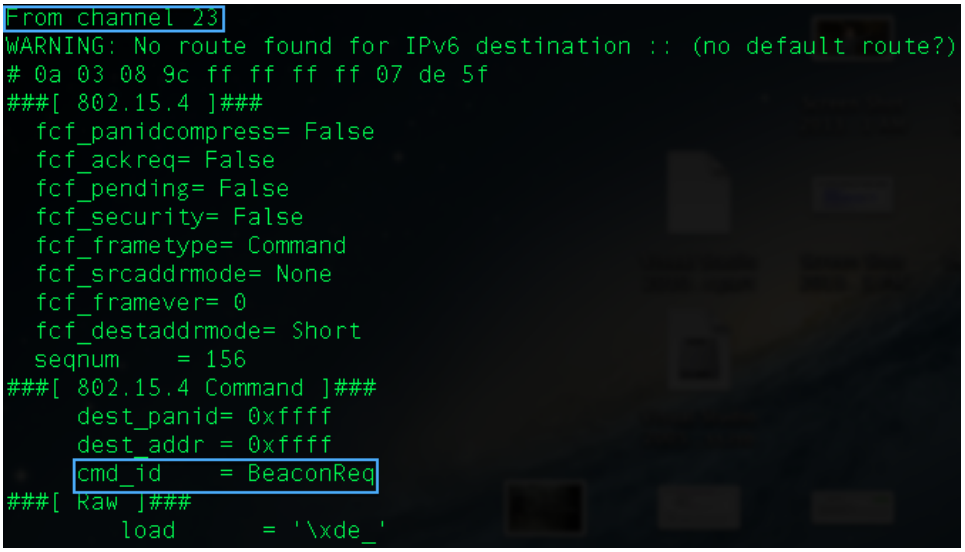


Figure 4.9: *Dissected beacon request to readable format*

4.2.2 Scenario 2:

In the second experiment, sniffing, capturing and replay attack were tested. The KillerBee device was implemented to dump the traffic flowing in the network in different formats. Figure 4.10 highlights the KillberBee *zbdump* command used to capture packets and number of packets captured.

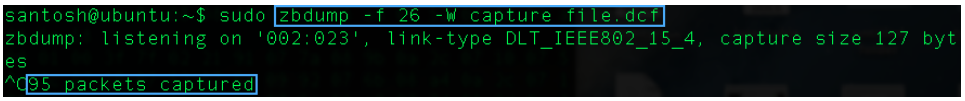


Figure 4.10: *Traffic captured through KillberBee zbdump command*

The captured packets were then resent in the network through another KillerBee command *zbreplay*. Figure 4.11 demonstrates the KillberBee command used and the packets resent in the network in channel number 12. The packets resent in the network was monitored through the Goodfet device. Figure fig:replayattack.png exhibits an instance of the packets resent from the attacking node that is KillerBee device. Similarly, *zbdsniff* command was executed to find out the network key as shown in Figure 4.13

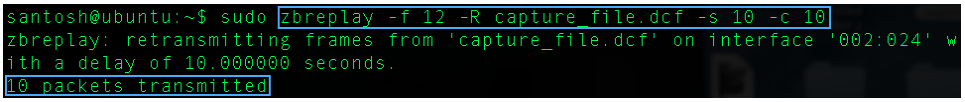


Figure 4.11: *Replay attack on channel 12*

4.2.3 Scenario 3:

The experimental setup for the scenario 2 was further extended for experimenting selective jamming attack on channel number 26. The replay attack made in the previous scenario was modified to insert huge amount

Figure 4.12: *Display of packet injected through replay attack*

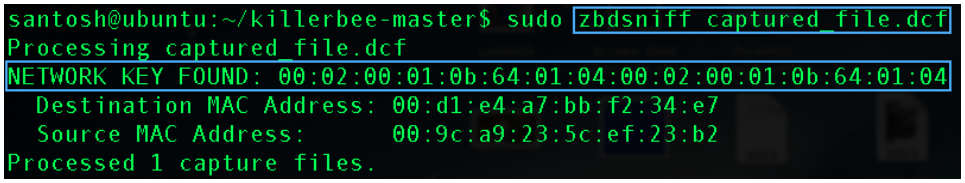


Figure 4.13: *Capturing of Network Key flowing in the network*

of traffic, in billions into the channel 26 of the network. Though it was for shorter time, the network seemed highly occupied by the replayed packets. There was great reduce in sent traffic from end devices. Figure 4.14 shows the reduction in sent packets due to selective jamming attack in channel 26.

4.3 Decoding of 802.15.4 traffic

In order to decode the sniffed traffic flowing in the above experiments for understanding and analyzing them, the Goodfet configured Telosb device and PPPSniffer configured Telosb device were used. The Telosb device with the Goodfet firmware would show decoded traffic through terminals as shown in Figure 4.9. The PPPSniffer firmware flashed Telosb device, on the other hand, operated as a bridge between 802.15.4 protocol and Wireshark. The PPPSniffer would feed data from 802.15.4 network to Wireshark and Wireshark would decode and dissect traffic into 802.15.4 format. An example of such traffic dissection through Wireshark is shown in Figure 4.15.

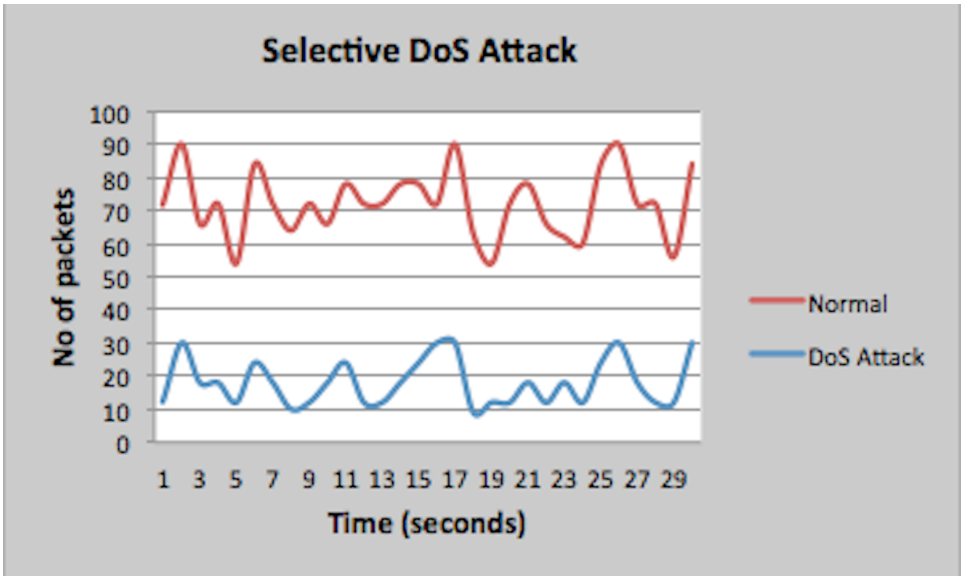


Figure 4.14: *Effect of selective jamming attack on 802.15.4 network*

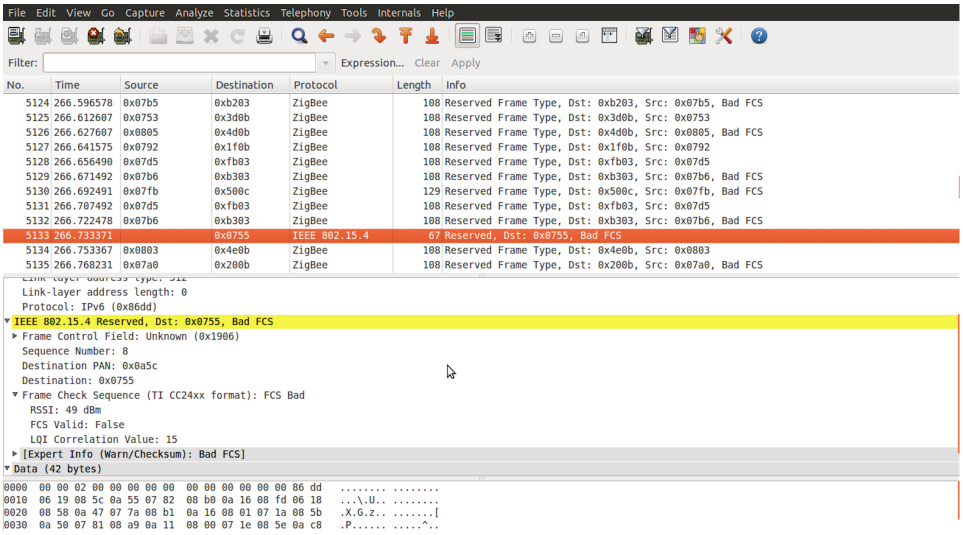


Figure 4.15: *Analysis of 802.15.4 traffic through Wireshark*

4.4 Analysis

This section presents the analysis of the result obtained from the above experiments. Analysis of the results is arranged in accordance with order of the experiments carried out above. Analysis is presented under similar headings as mentioned above to ease the task and also to provide a structure to analysis.

4.4.1 Experimental Setup I

The experiments; carried on in the OPNET simulator generated mostly expected results. However, some results obtained were unexpected. Details

are mentioned below:

Scenario 1:

When the network was designed to work in normal setup that is without any attacks or interference, the performance of the *Coordinator* node was smooth. There were no any packet losses in the network. In addition, the data sent from the *Coordinator* and other end sensor nodes were constant. This illustrated the smooth operation of ZigBee network as expected. However, as the load from one of the nodes (misbehaving node) was increased, the performance of the *Coordinator* was observed deteriorating as shown in Figure 4.4. As the data traffic from the misbehaving node went on increasing, the *Coordinator* started experiencing higher load and the *Coordinator* resource was consumed in handling those traffic in addition to normal traffic from the normal behaving sensor nodes. As a result, there was increase in load on *Coordinator* and degradation in the packets sent from the *Coordinator* in the network. However, when the parameters in the misbehaving node was altered to send around 40960 bits per second, the result obtained was quite unexpected but interesting. At that point, the load on the *Coordinator* started reducing as shown by Figure 4.5 . This is because, the misbehaving node has its own limitation. ZigBee devices are though designed to operate at low power, still may face energy problem if load on them are increased. The *Coordinator* device on the other hand is out of higher energy problem as the device is connected to the laptop. Hence, with increasing load on misbehaving node, might have increased the energy consumption. For this reason, the device might not have been able to generate constant load on the *Coordinator* till death. However, it could be confirmed if there had been provision of checking energy level of ZigBee end devices in the simulator.

Scenario 2:

With introduction of jammer node in the network, the result viewed was normal. As expected, there was loss in traffic sent from the *Coordinator*. This is because, the jammer node creates heavy traffic in the network. The objective of such traffic is just to occupy the channels preventing the data communication between end sensor nodes and the central *Coordinator* node. There was no change in data sent from the end devices. This might be because of jamming traffic wouldn't create load on end devices. These devices were set to send sensed data rather than receiving other data other than control information from *Coordinator*. However, as the data sent from end devices could not reach the destination *Coordinator* node, it had less data to respond with. Thus, there was reduction in follow-up traffic sent from the *Coordinator*.

4.4.2 Experimental Setup II

The physical experimental setup was quite complicated. It included different sensor devices and firmwares. Most of the results obtained were up to mark

while some of them were deviated. Analysis are presented in detail below:

Scenario 1:

In the first experiment, network scanning attack was tested. Through the KillerBee device, attempts were made to discover the PAN ids of the Shimmer devices and channel being used by them in the network. The KillerBee *zbstumbler* command was used for this purpose. The command would send the beacon request and would expect for the reply. Had the devices replied the beacon request, KillerBee device could identify PAN ids and the channel numbers. But, the Shimmer devices did not respond to the beacon request. This is because the Shimmer end devices could pair up with just single device and precisely based on MAC address. They would only respond to the network join command sent from *Coordinator*. However, when the network traffics were monitored through the Goodfet device, it showed that the broadcasted beacon request sent from the KillerBee device with the respective channels used as shown in Figure 4.8. To ensure that the highlighted traffics were beacon requests, embedded the Goodfet command was modified to operate in packet dissection mode. This made it possible to recognize the beacon requests. Figure 4.9 shows a dissected beacon request with respective channel used. This alerts that ZigBee network can be scanned and open the doorway for the attackers.

Scenario 2:

The real attack was tested in the second scenario. At first, the Goodfet *goodfet.ccspi surf* command was used to sniff the network traffic flowing on the network. It showed channel numbers along with traffic flowing on them. The KillerBee *zbdump* command which is analogous to *tcpdump* [8] was then executed to capture the traffic flowing in the channel 26 based on the information provided by the Goodfet device. The packets captured were then re-transmitted to the network in the same channel. However, to identify the attack, a replay attack was made on channel 12 and monitored from the Goodfet device as shown in Figure 4.12. ZigBee network has no security provision for replay attack [8]. This security weakness of the ZigBee network was taken into consideration to make the replay attack. Provided that ZigBee network transfers the OTA (over-the-air) key used for either encryption, decryption or joining the network over the air, KillerBee *zbdsniff* command could be used to sniff the such network keys. Figure 4.13 depicts a sample of captured OTA key flowing among the network traffic. The experiment was conducted on a externally pre-captured file as the Shimmer network under experiment would not transfer such keys over the air. It is inconvenient to flash such keys in every sensor nodes if the network contains thousands of sensor nodes. In such cases, the network keys might need to transfer over the air. This opens another doorway for attackers. However, in a small network concerning health system of a person, those keys can be flash individually in the end devices.

Scenario 3:

The selective DoS attack accomplished through extended replay attack provided inkling that through insertion of voluminous traffic interference can be created in the communication channels. Previously, it was found that the data communication between Shimmer sensor nodes and Shimmer *Coordinator* was taking place on channel 26. Therefore, KillerBee device was set to re-transmit billions of packets at interval of one packet per 0.001 second. The result showed that for certain period of time though short, such attack could consume the channel hugely, dominating data flow of the Shimmer end sensors. Thus, it was known that the selective DoS attack can easily be made once the channel used for data communication is figured out.

4.4.3 Decoding of 802.15.4 traffic

With use of bridging firmwares like the Goodfet and the PPPSniffer, 802.15.4 traffic could be decoded and dissected into human readable format. Generally, sniffers present data in hexadecimal format. To be these hexadecimal data human-readable, it needed to be decoded and dissected. With additional Scapy-dot15d4 plugin, the Goodfet firmware could present simple traffic dissection via terminal. It required some modifications in embedded coding to dissect traffic flowing in all communication channels for the Goodfet functionality. The PPPSniffer though took some time to get properly configured, efficiently fed the data to Wireshark. Wireshark has already been updated to support 802.15.4 traffic. The tool could decode and dissect 802.15.4 traffic at ground level. It could even show almost every information about the particular 802.15.4 frames and packets as shown in Figure 2.3. Thus, the combination of the PPPSniffer configured Telosb device and Wireshark could serve as efficient 802.15.4 packet analyzer.

Chapter 5

Discussion

This chapter highlights about the findings of this thesis work, significance of the findings and the experience and the knowledge gained. The chapter also mentions about how this work is similar to the previous work and how it differs from them on other hand. It provides briefing on how the preliminary plans and procedures were altered and why they were necessary. In addition, it enlightens about the limitation of the research work and the factors governing such limitations. At the end, the chapter provides overview on the possible extension for future students and scope for them in this field. The chapter is organized based on results obtained, procedures and approach followed, findings, scope and limitations, knowledge gained and future work.

In order to experiment the possibility of timely availability of data, different DoS attacks were carried out. Experiments were repeated time again to assure the reliability of the output. The results obtained from both simulation and physical lab exposed that the timely availability of data can be obstructed in the WBAN or ZigBee network. Such networks can be attacked with different forms of DoS attacks. Three forms of DoS attack were successfully experimented. In simulation work, jamming DoS attack and misbehaving node DoS attacks were successfully carried out while in physical lab selective jamming attack was accomplished. The study shows that life-critical data in e-health system undertaking via the WBAN or ZigBee network are susceptible to DoS attacks. In the physical lab, other attacks were experimented. Sniffing and replay attack were successfully tested. The WBAN or the ZigBee network can easily be scanned provided that there is availability of specific hardware and firmwares. The PPPSniffer and GoodFet open source firmwares can be flashed into the Telosb Tmote Sky device and operate as 802.15.4 network sniffer. Data traffic flowing in the network can be dissected into understandable format through packet dissector. Wireshark and scapy dot15d4 plugins are available for dissecting such traffics. It is ensured that ZigBee network has no security measure against replay attack. With use of KillerBee firmware flashed into Atmel AVR RAVEN RZUSBstick, replay attack is successfully carried out in the lab network.

However, certain attack like network scanning with beacon request broadcast cannot be accomplished in every 802.15.4 network as demon-

strated by previous works. The network sensors answer to beacon request only if they are configured to reply the beacon request of every devices in the network. But, it does not make any sense from security point of view to reply to any devices. The Shimmer sensor nodes in the physical lab is configured to communicate only with the *Coordinator*. Responses from the end sensors are dependent upon the MAC address of the *Coordinator* configured on them. Hence, network scanning made from KillerBee device cannot achieve successful result unless answering sensor devices are loosely configured.

It has been more than a decade that the WBAN technology has been developed. The survey conducted during research shows that the security system developed for the implementation of this technology is still in embryonic stage. Initially, the research was intended to conduct on comparative analysis of available adaptive intrusion detection and prevention systems for the WBAN security. Unfortunately, no such adaptive intrusion detection and prevention system tools were coined out. However, it has been a hot topic for research, and there has been a number of researches accomplished. A number of models for such tools have been proposed but very few such tools have been developed. The tools that have been developed so far for wireless intrusion detection system comes with specific device. For example, the CISCO has developed adaptive wireless intrusion detection and prevention system for WLAN. But, the software is embedded with the CISCO wireless devices. Hence, they are highly expensive. When it comes to the WBAN, almost no intrusion detection tool is found. The security system is mostly based on the WBAN applications themselves. However, Snort and Kismet were considered as intrusion detection tools for the thesis work. It is mentioned that with proper coding Snort could detect intrusions in the wireless system. In addition, Snort has plugin named WireSHnork for Wireshark. And Wireshark can dissect 802.15.4 traffic. Still as the Snort rules are developed for IP network, it cannot be directly applied for the WBAN. Therefore, it requires a emulator that can convert the WBAN traffic into IP network traffic so that Snort rules can be applied. The task might take longer time. Similarly, Kismet has developed a plugin named dot15d4 that facilitates the task of dissecting 802.15.4 traffic for Kismet. But, the plugin is still in rudimentary stage and can perform just simple tasks like packet sniffing. These circumstances restricted the intended goal of this thesis work. The work was thus confined within analysis of threats and could not carry out intended tasks on available security system like intrusion detection system.

Setting up proper experimental platform requires a bit more time. A number of simulation tools do exist, but most of them are deployed for finding out possible optimization of the network rather than security issues. Further, as the WBAN is new technology, most of these simulators do not have built in support for the WBAN. Those that support mostly lack graphical interface and others are found using additional externally developed models for the WBAN to carry on simulation work on it. Therefore, they might be deployed for general network testing in the WBAN. If non graphical tools are taken into consideration in order to create attack

scenario, one has to understand background coding and has to extend them. Thus, it might take longer time just to simulate attacks. For this reason, the OMNeT++ and the OPNET modeler were considered for simulation work. Both simulators can be run with free academic license. Initially, decision was made to work in the OPNET modeler. Thus, the license was ordered accordingly, but it would take 3-5 business days according to the OPNET company. Therefore, simulation work was continued with the OMNeT++ simulator. It does not support the WBAN directly but a model named MiXin can be implemented for the WBAN implementation. It is found that it requires creation of attack scenarios through coding despite the graphical support. Attempts were made to generate attacks but it was found time consuming to accomplish all intended simulation work. The option was then confined to the OPNET modeler. It took around 10 days to obtain license. The modeler supports ZigBee network but with limited functionality. This hindered to execute complete simulation work as planned. The simulator does not provide complete support for wireless PAN directly. The OPNET Wireless PAN model for Wireless PAN testing can be found for older version of the OPNET modeler but not for the recent version. Thus, creating DoS attacks through alteration of control messages of the WBAN protocol could not be accomplished.

Initially, plan was made to work on just Shimmer devices, which were previously present in the ASSET lab. The communication with Shimmer Company support personnel had provided possible deployment of the Shimmer devices to execute planned experiments. The modifications on firmwares developed for other similar standard devices could possibly be used. With time, it was known that Shimmer devices application could easily be deployed to establish the WBAN standard network, but it was hard to configure them as attacking nodes. Thus, the physical lab setup to carry on intended experiments on the WBAN technology required different additional sensor devices. These sensor devices are not easily available in local market and thus were ordered from different countries. Likewise, the firmwares to be configured in these devices are also rare. A number of open source firmwares have been developed, but most of the firmwares are device specific. Thus, it requires to have sound knowledge about compatible hardware and firmwares. For absolute use of KillerBee device for different attack scenarios, it requires special hardware and firmware to flash KillerBee firmware in Atmel AVR RAVEN RZUSBstick. Such device is expensive. Therefore, the device was sent to the developer of the KillerBee to flash it with KillerBee firmware.

Most of the previous works are limited to security exploitation in the WBAN. These works are generally carried on simulators probably due to difficulty in obtaining the required hardware. The simulation work of the research is not different from that of previous work. It could be taken forward if other simulation tool that supported Wireless PAN simulation was considered. Benchmarking the resource consumption like monitoring battery consumption would provide evidence to make clear decisions. The OPNET modeler does not provide platform for analyzing undergoing network traffic. Unlike previous work, this thesis work has proved that network scanning

with beacon request broadcast can generate no result unless the protocol is loosely configured. Even default configuration of the recent WBAN application nullifies the gain of network scanning with beacon request. This work goes ahead of the previous work with physical lab experiments where network traffic can be analyzed. No new firmwares are developed for the experiments. However, modification on firmwares are made where ever needed. Initially, the PPPSniffer could dissect package flowing on only channel 11, but it was modified to dissect packets flowing on every communication channels. Likewise, configuration of the Goodfet device in TelosB device did not work straight forward as guided by the Goodfet tutorial. It requires some modifications to configure properly and run the commands. The thesis provides idea of how different hardware and firmware can be grouped together to work as a complete package for the WBAN implementation and conducting security experiments on them. For this reason, the research provides a ground for switching the approach for implementing the WBAN experiments on real devices for those who intend to work on simulators.

Despite the thesis has been hindered by different problems, it has produced different results. It has demonstrated different techniques that an intruder might come up with to create obstructions in data communication between sensor nodes. It is shown that techniques behind creation of DoS attacks are not complex. But, the effects of such attacks may matter significantly. In relation to health system, such hindrance in data communication might be paid with patient lives. Similarly, the research has demonstrated that 802.154.4 network can easily be sniffed. This alarms for the prompt necessity of a system to prevent intruders from entering into the network and sniff the packets. It also exhibits the possibility of capturing and re-transmitting the packets into the network. The packet re-transmission might cause severe result as well. For simple example, a packet containing information about blood sugar level can be taken. Suppose, the packet contains information stating that sugar level is normal, and is transmitted over and again. The situation might be critical when packet containing normal sugar level is transmitted when the sugar level goes beyond threshold. Obviously, patient life is endangered. If the tests are conducted in commercial applications, viability of replay attacks and the possible effects might be brought out with proper evidence. The result also bolsters that, if the network key is configured to send over the air, it might be captured . This network key might be used to decrypt the captured packets. Therefore, confidentiality of the data might be breached. This thesis provides concept of different commonly used hardware and firmwares, configuration issues and overview of their deployment for different purposes. Hence, it assists people in saving their valuable time in gathering knowledge about such devices and firmwares and their precise implementation technique.

The experiments were conducted on Shimmer sensor network and specific application was deployed for communication among the network nodes. As most of the open source firmwares developed for sensor devices are device specific, these firmwares are not compatible with Shimmer Device.

This restricted flexibility of working with device and conduct variety of experiments. The thesis work could have generated more convincing results if the experiments were conducted in devices like Telosb Tmote Sky instead of Shimmer devices. This is because Telosb devices can be configured with different types of open source firmwares. It is comparatively easier to alter the functionality of the device through modification on firmwares. Thus, these devices can be made to work to fulfill different needs. Further, it would have saved more time for experiments on physical lab if the experiments on simulators were not thought of. Experiments conducted and experimental results obtained are not different from the previous works. However, simulation work assists in understanding functionality of the WBAN technology. Thus, it contributes significantly in designing the lab setup and predicting the results.

While conducting this research, some complexions were encountered due to overlooking infrastructure setup complications. It was clear that the implementation of the WBAN technology requires working with different sensor devices. These devices are not commonly used, so it requires in-depth survey in the very beginning. In contrary, most of the time was spent on literature review. The literature review had warned about unavailability of security tools and complications that might encounter during physical lab set up. The lab devices were already present in the lab, so such warnings were overlooked. Most of the previous works were based on simulation work, therefore it could be inferred that simulation tools were easily available and could easily be deployed. Ironically, obtaining the OPNET modeler was time consuming and was found unable to get deployed as expected. The simulation tools are quite sophisticated and thus it needs some time to understand the functionality of the tools. Since, the simulation results are not different from that of previous work, it would have been wise to utilize the time spent on simulation work over physical lab work. In lab work, as mentioned previously, it was thought to alter the firmware that was being used on Shimmer nodes to make it operate as desired based on literature review. Later it was found that the modification task is quite complicated and thus suggested the need of other simple applications. But, there exists very few open source ZigBee applications that could be used in Shimmer nodes. Most ZigBee applications come with pre-installed on devices. Thus, most of the experiments were limited to physical and data link layer of 802.15.4 network. It requires extensive preliminary survey while working on new technology like the WBAN. The alternative approaches should be planned in advance to bypass different hindrances that might be encountered due to unavailability of firmwares and hardware.

The thesis provides quick knowledge about the WBAN technology, some associated devices and their purpose and functionality. It delivers knowledge about different platforms for playing with the WBAN implementation. More importantly, it disseminates knowledge about findings and further requirements in this field in terms of security system specifically in e-health system. The work has shown that the WBAN technology is vulnerable to different attacks. Ironically, the technology lacks efficient security system. In fact, the security system developed till now are mostly confined as paper

work only. Mostly, the models have been developed. The security tools, which have been developed are found used only for the research purpose. But, the security requirement in the WBAN application specially in the field of e-health system is extremely important. Through the simulation work and physical lab work, different types of attacks have been successfully made. The previous works are mostly performed in simulators. The research has shown that different attacks can also be generated in physical lab setup with devices like the Telosb and the AVR RAVEN, and the firmwares like the Goodfet and the KillerBee. For analysis, Scapy plugin dot15d4 can be embedded with the Goodfet. Similar, the PPPSniffer can be configured to feed the WBAN traffic to Wireshark. Using these hardware and software one can easily setup own 802.15.4 network and continue exploring security issues. Kismet has initiated developing plugin for 802.15.4 intrusion detection. Since, the plugin is still in rudimentary stage, one think of enhancing the plugin. One can work on developing a bridge between the WBAN and the WLAN protocols so that the WBAN traffic can be emulated into data traffic understandable by WLAN security system. As a result, with some modification on tools like Snort and their intrusions detection rules, it might detect intrusions in the WBAN. With use of firmwares like the PPPSniffer and the WSbridge, certain sensor devices can feed the WBAN traffic to Wireshark packet analyzer. Further, Snort plugin named WireSHnork has been developed for Wireshark. This provides some motivation and hope for using Snort as intrusion detection in the WBAN. One can think of contributing with developing security system for the WBAN based on these tools. This thesis is based on self configured devices. One of the interesting future work can be testing the attacks discussed on this work and also other forms of attacks on commercial ZigBee devices. However, as the devices needed for experiments are not easily available, time constraint should be considered if one thinks of starting from scratch, else, the work can be further extended and effort can be made to develop a security tool for the WBAN implementation. Security tools for the WBAN are rare but extremely important. Hence, even a small contribution will definitely be highly appreciated.

Chapter 6

Conclusion

This thesis has been conducted as the requirement for the completion of Master's Degree program in *Network and System Administration* at University of Oslo. It has been carried on as a part of ASSET project. The study has researched on security system that is currently available for the WBAN implementation. The core focus was paid on ZigBee technology. The overall task was carried out in two parts: Simulation work and real hardware work. DoS attacks like *Jamming Attack* and *Misbehaving Node Attack* were experimented successfully in simulator. Likewise, *Selective Jamming DoS Attack, Sniffing, Packet Capturing and Replay Attack* were shown possible through lab work.

It has been demonstrated that traditional network scanning tools like *KillerBee* might not find out the identity of network elements in the WBAN sensor network. However, *KillerBee* was an efficient firmware available to create different types of attacks in 802.15.4 and ZigBee network. Similarly, *Goodfet* and *PPPSniffer* (together with *Wireshark*) were equally efficient tools to analyze the WBAN traffic. *Telosb Tmote Sky* was found multipurpose device to carry on experiments on the WBAN security. *Scapy* was fine tool to decode and dissect the WBAN traffic. The research could not accomplish the overall intended tasks. No Intrusion Detection System was found developed for the WBAN. The task carried on simulation work could be accomplished in physical lab with some modification on firmwares deployed for sensor nodes. It would have generate more convincing results if the time utilized for simulation work was paid to lab work. The time could be utilized to get familiarized with application code and modify them accordingly to create more attacks for security analysis.

In addition to delivering knowledge about generating different attacks on the WBAN deployment, this thesis contributes on setting up the WBAN lab for experimenting security tests. The research points out the lack of security system tools in realm of the WBAN technology deployment despite its increasing demand. It can be extended forward with an attempt to develop a tool that might mitigate above mentioned attacks. *Kismet dot15d4* is an open source security tools for the WBAN which is under development. The project can be carried on to develop a security system from such rudimentary tool and make important contribution in the WBAN. The thesis

was based on customized the WBAN devices. In future, experiments can also performed on commercial the WBAN application to analyze the security system present on commercial products. This will help understand and get familiarized with current security system in the WBAN which are added in these commercial products.

Bibliography

[1] M. Osborne. Widz - the wireless intrusion detection system. http://www.loud-fat-bloke.co.uk/articles/widz_design.pdf, 2012. updated on 03/02/2013.

[2] Daintree Networks. Getting started with zigbee and IEEE 802.15.4. *ZigBee Security*, pages 1–26, 2010.

[3] M. Pihelgas. A comparative analysis of open-source intrusion detectioin systems. Master's thesis, Tallinn University of Technology, Tallin, Estonia, 2012.

[4] Lehigh University. Wireless standards. http://www.lehigh.edu/wireless/standards.shtml, 2012. updated on 23/02/2013.

[5] S. Poslad W. Leister, H. Abie. Defining ASSET scenarios. *Norsk Regnesentral 2012 17 s*, 2012.

[6] H.J. Yoo and A. Burdett. Es4: Body area network: Technology, solutions, and standardization. In *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2011 IEEE International*, pages 531–531, Feb.

[7] S. S. Jung. Attacking and securing beacon-enabled 802.15.4 networks. Master's thesis, Georgia State University, Georgia,USA, 2011.

[8] J. Wright. Killerbee, practical zigbee exploitation framework. http://blip.tv/source-boston-2010/josh-wright-killerbee-practical-zigbee-exploitation-framework-3586816, 2010.

[9] Google Project Hosting. Killerbee, framework and tools for exploiting zigbee and IEEE 802.15.4 networks. https://code.google.com/p/killerbee/, 2010. updated on 27/07/2012.

[10] G. Zhou A. Wood, J.A. Stankovic. Deejam: Defeating energy-efficient jamming in ieee 802.15.4-based wireless networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON 07. 4th Annual IEEE Communications Society Conference on*, pages 60–69, 2007.

[11] C.P. O'Flynn. Message denial and alteration on ieee 802.15.4 low-power radio networks. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, pages 1–5, 2011.

[12] J. M. Gonzalez de Jesus. Exploring jamming attacks using opnet 12.0. Master's thesis, University of Pittsburgh, Pittsburgh,PA,USA, 2007.

[13] A. Ghosh K.C. Doddapaneni. Analysis of denial-of-service attacks on wireless sensor networks using simulation. http://kaspersky.com, 2010.

[14] K. Srinivasan E.M. Belding-Royer R.A. Kemmerer V. Giovanni, S. Gwalani. An intrusion detection tool for aodv-based ad hoc wireless networks. In *Computer Security Applications Conference, 2004. 20th Annual*, pages 16–27, 2004.

[15] N. Bourdriga. *Security of Mobile Communication.* Auerbach Publications, New York, USA, 2009.

[16] Radio-Electronics.com. Wireless technologies, 802.11 standards tutorial. http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php, 2013. updated on 08/03/2013.

[17] AirDefense Inc A. Khatod. Five steps to WLAN security: A layered approach. http//:www.computerworld.com/s/article/97178/Five_Steps_To_WLAN_Security_A_Layered_Approach, 2004. updated on 17/01/2013.

[18] M. Reeve C. Maple, H. Jacobs. Choosing the right wireless lan security protocol for the home and business user. pages 8 pp.–, April.

[19] Gunter Schafer. *Security in Fixed and Wireless Network.* John Wiley and Sons, Ltd, The Atrium, Southrn Gate, Chichester, West Sussex, England Publications, New York, USA, 2003.

[20] B. Samadi A.H. Lashkari, M.M.S. Danesh. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). In *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 48–52, Aug.

[21] K. Sinha S. Maitra B. Sinha S. Sen Gupta, A. Chattopadhyay. High performance hardware implementation for rc4 stream cipher. *Computers, IEEE Transactions on*, PP(99):1–1, 2009.

[22] S. Riley K. Tewson. Security watch: A guide to wireless security, 2008.

[23] R. Ahmad S.N. Ramli. Surveying the wireless body area network in the realm of wireless communication. In *Information Assurance and Security (IAS), 2011 7th International Conference on*, pages 58–61, Dec.

[24] R. Sivakumar M. Somasundaram. Security in wireless body area networks: A survey. *ipcsit.com*, 2011.

[25] S. Saleem, S. Ullah, and Kyung-Sup Kwak. Towards security issues and solutions in wireless body area networks. In *Networked Computing (INC), 2010 6th International Conference on*, pages 1–4, May.

[26] L. Xiaohui M. Barua, M.S. Alam and X. Shen. Secure and quality of service assurance scheduling scheme for wban with application to ehealth. In *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, pages 1102–1106, March.

[27] Y.B. Choi T. Lakshman S. Lim, T. H. Oh. Security issues on wireless body area network for remote healthcare monitoring. In *Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on*, pages 327–332, June.

[28] N Ullah K. Kwak, S. Ullah. An overview of IEEE 802.15. 6 standard. *Applied Sciences in Biomedical, arXiv:1102.4106v1 [cs.NI], available at : http://arxiv.org/pdf/1102.4106.pdf*, 2010.

[29] ZigBee Alliance. Zigbee. http://www.zigbee.org/Home.aspx, 2013. updated on 2013.

[30] Inc. OPNET Technologies. Opnet modeler wireless suite. http://www.opnet.com/. updated on 2013.

[31] Integration Assosiate I. Marsden. Network layer overview. 2006.

[32] Wireless Sensor Network Research Group D. Gascon. 802.15.4 vs zigbee. http://www.sensor-networks.org/?page=0823123150, year = 17/11/2008, note = updated on 2013.

[33] F. Yu Y. Liu. Immunity-based intrusion detection for wireless sensor networks. In *Neural Networks, 2008. IJCNN 2008. (IEEE World Congress on Computational Intelligence). IEEE International Joint Conference on*, pages 439 –444, june 2008.

[34] A. Zainal M. A. Rassam, M.A. Maarof. A survey of intrusion detection schemes in wireless sensor networks. *American Journal of Applied Sciences*, 2012.

[35] M. Ahmed-Nacer H. Bensefia. Towards an adaptive intrusion detection system: A critical and comparative study. In *Computational Intelligence and Security, 2008. CIS 08. International Conference on*, volume 2, pages 246 –251, dec. 2008.

[36] V. Marinova-Boncheva. A short survey of intrusion detection systems. *Institute of Information Technologies, 1113 Sofia*, pages 23 –29, 2007.

[37] Red Hat. *Security Guide, Chapter 9. Intrusion Detection.* Red Hat Enterprise Linux 4.5.0, 2007.

[38] L. Deng and D.Y. Gao. Research on immune based adaptive intrusion detection system model. In *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC 09. International Conference on*, volume 2, pages 488 –491, april 2009.

[39] M. Gao and J. Tian. Wireless sensor network for community intrusion detection system based on improved genetic algorithm neural network. In *Industrial and Information Systems, 2009. IIS 09. International Conference on*, pages 199 –202, april 2009.

[40] S. Goyal P. Jain. An adaptive intrusion prevention system based on immunity. In *Advances in Computing, Control, Telecommunication Technologies, 2009. ACT 09. International Conference on*, pages 759–763, Dec.

[41] Z.D. Zhong G. Yi W. A. Lee S. Stolfo E. Eskin, M. Miller. Adaptive model generation for intrusion detection systems. *Department of Computer Science Columbia University*, pages 1 – 14, 2000.

[42] M. Imran S.Rajasegarar C. O'Reilly, A. Gluhak. Online anomaly rate parameter tracking for anomaly detection in wireless sensor networks. In *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on*, pages 191–199, June.

[43] Rahul Khanna and Huaping Liu. System approach to intrusion detection using hidden markov model. In *Proceedings of the 2006 international conference on Wireless communications and mobile computing*, IWCMC 06, pages 349–354, New York, NY, USA, 2006. ACM.

[44] Snort Project. Snort faq. //http://www.snort.org/snort/faq/, 2013. updated on 2013.

[45] Snort Project. Snort users manual 2.9.4. http://manual.snort.org, 2013. updated on 2013.

[46] A. Lockhart. Snort wireless, howpublished = http://www.snort-wireless.org/, year = 2005.

[47] Open Information Security Foundation. Suricata, open source ids / ips / nsm engine. http://suricata-ids.org/, 2013. updated on 06.03.2013.

[48] OSSEC Project. Ossec - open source security. //http://www.ossec.net, 2013. updated on 03.11.2012.

[49] IBM. Ossec: The open source intrusion prevention system. https://www.ibm.com/developerworks/mydeveloperworks/blogs/6e6f6d1b-95c3-46df-8a26-b7efd8ee4b57/entry/ossec_the_open_source_intrusion_prevention_system49?lang=en, 2013. updated on 2013.

[50] The Bro Project. The bro network security monitor. //http://bro.org/index.html, 2012. updated on 2012.

[51] Security Advancements at the Monastery John Gerber. Three open source IDS/IPS engines: The setup. http://blog.securitymonks.com/, 2010. updated on 2013.

[52] Inc Tripwire. Tripwire: A history of security and innovation. http://www.tripwire.org/, 2011.

[53] Akadia. Intrusion detection with tripwire. http://www.akadia.com/services/tripwire.html. Last visited on 10/02/2013.

[54] Inc Sourcefire. Next-generation intrusion prevention system (NGIPS). http://www.sourcefire.com/security-technologies/network-security/next-generation-intrusion-prevention-system, 2013.

[55] Cisco. Cisco adaptive wireless ips software. http://www.cisco.com/en/US/products/ps9817/index.html, 2013.

[56] Mike Kershaw. Kismet. http://www.kismetwireless.net/documentation.shtml, 2011. last updated 08/03/2013.

[57] Aroba Networks. Rfprotect wireless intrusion protection. http://www.arubanetworks.com/products/arubaos/rfprotect-wireless-intrusion-protection. last updated 2013.

[58] Fei Yu. A survey of wireless sensor network simulation tools. *http://www1.cse.wustl.edu/ jain/cse567-11/ftp/sensor/index.html*, pages 1–10, 2011.

[59] ns-users@isi.edu ns. Widz : The wireless intrusion detection system. http://www.isi.edu/nsnam/ns/. updated on 2013.

[60] UCLA Compilers Group. Avrora, the AVR simulation and analysis framework. http://compilers.cs.ucla.edu/avrora/, 2008. updated on 17/12/2013.

[61] OMNeT Community. Omnet++. http://www.omnetpp.org//, 2001. updated on 2013.

[62] Y.B. Woldergiorgis P.A. Floor I. Balasingham W. Leister, H. Abie. Defining ASSET lab. *Norsk Regnesentral 2012 43 s*, 2012.

[63] Shimmer Research. Products. http://www.shimmer-research.com/, 2008. last updated 2013.

[64] ADVANTICSYS. Products, CM 5000. http://www.advanticsys.com/. last updated 2013.

[65] ATMEL Corporation. Atmel AVR2016: RZRAVEN hardware user guide. http://www.atmel.com/, 2012.